

**National Security Archive Cyber Vault**  
**A CHRONOLOGY OF THE CYBER ASPECTS**  
**OF THE WAR IN UKRAINE<sup>1</sup>**

(As of May 30, 2023)

**PRE-2021 EVENTS**

2010-2020 – (Approx.) Russia undertakes a long-term effort to build up its ability to control access to the Internet within the country. Activities include developing legal measures and expanding infrastructure such as creating content filters and block lists and installing ways to administer oversight within telecommunications firms.

([Russia Takes a Big Step Toward Internet Isolation | WIRED](#))

According to Stanislav Shakirov, cofounder of the Russian digital rights group Roskomsvoboda and founder of Privacy Accelerator, Russia has been following five basic principles, reports *Wired*:

- Control the internet infrastructure (by owning internet cables, e.g.)
- Pressure websites and internet companies to censor content
- Ban independent media organizations and enforce the “foreign agents” law
- Induce self-censorship and reluctance to take part in protests
- Block websites through legal and technical means

([Russia Is Quietly Ramping Up Its Internet Censorship Machine | WIRED](#))

2014 – A coordinated cyberattack targets Ukraine’s Central Election Committee and media sector. CrowdStrike later attributes the hit to BERSERK BEAR, described as an “adversary group believed to be related to the FSB.” (House Homeland Security Subcommittee on Cybersecurity, Infrastructure Protection and Innovation, hearing on Russian cyber threats, 4-5-22)

2014 – According to *Wired* (2022), “In 2014 the security firm FireEye had issued warnings about a team of hackers that was planting BlackEnergy malware on targets that included Polish energy firms and Ukrainian government agencies; the group seemed to be developing methods to target the specialized computer architectures that are used for remotely managing physical industrial equipment. The group’s name came from references to Dune found buried in its code, terms like Harkonnen and Arrakis, an arid planet in the novel where massive sandworms roam the deserts.” ([Russia's Cyberwar on Ukraine Is a Blueprint for What's to Come | WIRED](#))

---

<sup>1</sup> © The National Security Archive Fund, Inc., 2023. Reuse for educational, non-commercial, non-political purposes is permitted. DISCLAIMER: Entries are summaries, paraphrases or quotations from original sources. Dates and quotations are as precise as possible, but accuracy of original source content has *not* been independently verified. Source credit is provided along with clickable links to original materials, though links may become outdated over time. Entries are derived from government documents, news outlets, commercial firms, and social media posts. Inclusion is not an endorsement in any respect nor a guarantee of reliability. Compiled by Malcolm Byrne with Bridget Sullivan.

July 11, 2014 – According to a 2022 article describing early Russian cyber activities in Ukraine: “On July 11, 2014, in the town of Zelenopillya, roughly five miles from the Ukrainian border with Russia, the brigade had planned to sever the supply line of the Donbas separatists when electronic warfare caught them by surprise. Witnesses described the scene to me: First there came the humming of an unmanned aerial vehicle able to clone cellular networks to locate active cellphones, followed by cyberattacks against Ukrainian command and control systems. Their communication systems disabled, Ukrainian forces were unable to coordinate with one another. Then, short-range rocket systems from inside Russia disabled two battalions, including T-64 tanks and amphibious tracked vehicles. Three trucks carrying troops exploded. Stumbling from the transport, one soldier clutched his entrails, and shouted for his mother. The attack killed 30 Ukrainians and wounded hundreds and lasted roughly two minutes.” ([‘Kill Your Commanding Officer’: On the Front Lines of Putin’s Digital War With Ukraine - POLITICO](#))

December 10, 2014 – CISA sends out an alert: “ICS-CERT has identified a sophisticated malware campaign that has compromised numerous industrial control systems (ICSs) environments using a variant of the BlackEnergy malware. Analysis indicates that this campaign has been ongoing since at least 2011.” A later alert indicates the same malware causes the December 23, 2015, Ukraine power outages. In this case, affected entities include American power and water utility networks. FireEye identifies the GRU-connected group Sandworm as the perpetrators. The discovery worries U.S. experts because it shows the group is targeting entities in the United States. ([Ongoing Sophisticated Malware Campaign Compromising ICS \(Update E\) | CISA](#); [Russia's Cyberwar on Ukraine Is a Blueprint for What's to Come | WIRED](#))

2014 on – According to a 2022 news article describing early Russian cyber activities in Ukraine: “Ukrainian officials and soldiers said they have tightened the security of their internal communications since 2014, like with the incorporation of L3Harris secure handheld radios sent by NATO and the U.S., [but] vulnerabilities remain. Meanwhile, the Russian military has relocated more electronic warfare equipment to the borders with Ukraine, such as the Leer-3 RB-341V, a drone-based system that can monitor cellular and data transmission networks, suppress wireless communications, locate electromagnetic emission sources and even send text messages to front-line soldiers. The Ukrainian military has little equipment that can replicate or fight back against these attacks.” ([‘Kill Your Commanding Officer’: On the Front Lines of Putin’s Digital War With Ukraine - POLITICO](#))

September 2, 2015 – Russian Federal Law No. 242-FZ goes into effect, requiring parties operating within Russia which collect personal data from Russian users of the Internet to store that information on servers located inside the country. ([3 Things To Know About Russia's New Data Localization Law - Law360](#); [Encrypt your data to make GDPR and Russian Data Localization Law compatible \(iapp.org\)](#))

December 23, 2015 – Hackers mount a sophisticated attack on three electrical power distribution centers in Western Ukraine, ultimately taking some dozens of substations offline and leaving more than 230,000 residents without power. They also disable backup power supplies to two of the centers. Ukrainian authorities blame Russia; in July 2021, CISA finally concurs. (ICS-CERT Alert (IR-ALERT-H-16-056-01), 2-25-2016; [Inside the Cunning, Unprecedented Hack of Ukraine's Power Grid | WIRED](#); [Cyber-Attack Against Ukrainian Critical Infrastructure | CISA](#))

Some experts point out that this amounts to a rare case of a hacking incident against an industrial control system (ICS) having an impact on ordinary citizens. ([Russian hackers suspected in attack that blacked out parts of Ukraine - The Washington Post](#))

According to a later analysis, “What was striking about this particular attack is that the three grids were disabled within a half hour of each other. The grids were unconnected, and so these breakdowns were not the result of cascading failures, a not-uncommon situation for power grids. Thus this attack demonstrated an unexpected level of capability – by Russia or others. Launching such nearly simultaneous attacks against three distribution networks that each operated somewhat differently had not been anticipated by the U.S. It was a wake-up call for the U.S. Department of Homeland Security, which worked to develop greater resiliency in the nation’s power grids.” ([Cyberwar in Ukraine: What You See Is Not What’s Really There - Lawfare \(lawfareblog.com\)](#))

2016 – According to a USAID release in 2022: “In 2016, USAID launched the nine-year, \$81 million Ukraine Responsive and Accountable Governance Program to promote citizen-centered elections and political processes in Ukraine. Under the activity’s cybersecurity component, USAID partners with Ukraine’s Central Elections Commission (CEC) to strengthen its cybersecurity capacity and counter growing online threats to electoral systems.” ([Cybersecurity Fact Sheet | Ukraine | U.S. Agency for International Development \(usaid.gov\)](#))

2016 – Russia blocks access to LinkedIn from inside the country. ([Encrypt your data to make GDPR and Russian Data Localization Law compatible \(iapp.org\)](#))

December 17, 2016 – Sandworm, a Kremlin-backed hacker group, uses malware named CrashOverride or Industroyer to hit a single electrical transmission level substation at the Ukrenergo utility in Ukraine. The attack uses a known vulnerability in its Siemens SIPROTEC relays. According to Dragos, “The most important thing to understand ... from the evolution of tradecraft is the codification and scalability in the malware towards what has been learned through past attacks. The malware took an approach to understand and codify the knowledge of the industrial process to disrupt operations as STUXNET did.” This is reported to be the first case of malware “in the wild” that can cause blackouts through direct interaction with electric grid equipment. Dragos notes: “It marks an advancement in capability by adversaries who intend to disrupt operations and poses a challenge for defenders who look to patching systems as a primary defense, using anti-malware tools to spot specific samples, and relying upon a strong perimeter or air-gapped network as a

silver-bullet solution.” ([CrashOverride revised091118 \(dragos.com\)](#); [Building a Cyber Force Is Even Harder Than You Thought - War on the Rocks](#); [Russia's Sandworm Hackers Attempted a Third Blackout in Ukraine | WIRED](#))

December 29, 2016 – The White House releases a statement by President Obama detailing a number of measures the U.S. will be taking in response to Russian election interference. The statement wraps up with an intentionally vague comment: “These actions are not the sum total of our response to Russia’s aggressive activities. We will continue to take a variety of actions at a time and place of our choosing, some of which will not be publicized.” The *Washington Post* later reports that these additional measures include certain cyber activities. One is “designed to be detected by Moscow” and mainly intended to show the extent of U.S. reach. A second comprises a new covert program by the NSA, CIA, and U.S. Cyber Command that involves deploying “implants” inside Russian networks that can be activated remotely in case Russia chooses to conduct future aggressive acts, the newspaper reports. The mid-2017 report finds no indication the Trump administration has done anything to stop the program. ([Obama’s secret struggle to retaliate against Putin’s election interference - Washington Post](#))

2017 – The long-standing issue of cybersecurity insurance experiences some significant moments this year. A 2022 article notes that cybersecurity insurance has been around since the early 2000s at least, mostly focusing on events like data breaches and subsequent lawsuits and regulatory action. According to CyberScoop, “That changed rapidly in 2017 when the [WannaCry](#) and [NotPetya](#) attacks showed how quickly a cyberattack could have resounding consequences around the globe. Then came [another crisis moment](#) for the industry: a rapid rise in ransomware attacks and an increase in ransomware demands, including a high-profile [ransomware attack on U.S. fuel provider Colonial Pipeline](#).” ([The cyber insurance market has a critical infrastructure problem \(cyberscoop.com\)](#))

2017 – 2022 – According to a May 2022 State Department release:

“DOE [Department of Energy] has a long-standing relationship with the energy sector in Ukraine, including work with Ukrainian utilities to help enhance their cybersecurity posture. In the leadup to Russia’s further invasion of Ukraine, DOE, leveraging the expertise of our National Labs, worked with utilities to focus on potential near-term cybersecurity enhancements, while also continuing our work on long-term resilience efforts.

“The Treasury Department has worked with the National Bank of Ukraine (NBU), via the Software Engineering Institute (SEI), to support NBU’s Computer Security Incident Response Team (CSIRT) to improve cybersecurity information sharing in Ukraine’s financial services sector. Leading up to Russia’s further invasion of Ukraine, Treasury offered NBU assistance on specific cybersecurity issues while continuing to work on longer-term cybersecurity projects to better ensure the cyber resilience of Ukraine’s financial sector ([U.S. Support for Connectivity and Cybersecurity in Ukraine - United States Department of State](#))



June 27, 2017 – Ukraine’s state-owned Oschadbank, one of the largest banks in the country, sustains a major attack later dubbed “NotPetya.” NATO Cooperative Cyber Defence Centre of Excellence experts conclude the perpetrator was “probably ... a state actor or non-state actor with support or approval from a state.” Legal scholars later cite the incident as an illustration of “the complexity of applying international law to factually ambiguous cyber scenarios.” ([The day a mysterious cyber-attack crippled Ukraine - BBC Future](#); [The NotPetya Cyber Operation as a Case Study of International Law – EJIL: Talk! \(ejiltalk.org\)](#))

According to the GAO later: “Specifically, the GRU compromised the development environment of a Ukrainian company that produces tax accounting software to deploy malware on systems where the software was installed. After NotPetya infected a machine on which that software was installed, it was capable of automatically spreading through a network and infecting other machines. NotPetya spread worldwide, damaged computers used in critical infrastructure, and is estimated to have caused about \$10 billion in damages globally.” (GAO, “Cyber Insurance: Action Needed to Assess Potential Federal Response to Catastrophic Attacks,” June 2022)

Victor Zhora, deputy chairman of Ukraine’s State Service of Special Communications and Information Protection, says later the NotPetya attacks are a “critical turning point” for Ukraine’s cyber defense development. ([Battling Moscow's hackers prior to invasion gave Kyiv 'full dress rehearsal' for today's cyber warfare \(cyberscoop.com\)](#))

July 30, 2017 – Putin signs new legislation banning VPNs and other means of gaining anonymous access to the Internet. ([Putin passes law that will ban VPNs in Russia | TechCrunch](#))

2018 – late 2022 – During this period, USCYBERCOM conducts “thirty-seven operations, twenty nations, on fifty-five different networks,” according to Gen. Paul Nakasone. According to a media report, the aim is “to help partner nations shore up their cyber defenses against threats ... These so-called hunt forward operations involve physically sending defensively oriented cyber protection teams from the Cyber National Mission Force to foreign nations to hunt for threats on their networks at the invitation of host nations.” The article, in CyberScoop, goes on: “A Cyber National Mission Force spokesperson clarified to FedScoop that there have been 27 total hunt forward operations since 2018, though most of them have occurred since the COVID-19 pandemic in March 2020. They also added that these were 27 separate deployments to 15 nations, including Montenegro, Estonia and North Macedonia, though some deployments were to the same nation multiple times.” ([Cyber Command has deployed to nations 27 times to help partners improve cybersecurity \(fedscoop.com\)](#))

USCYBERCOM head Paul Nakasone ups these figures at a July 2022 public conference: he counts 50 different hunt forward operations across 16 countries in the past three years. “This is a growth industry for us,” he says. “We are also positioning ourselves to understand our adversaries better.” ([Cyber Command chief](#)

[stands by comments on 'offensive' operations against Russia - The Record by Recorded Future\)](#)

Winter 2018 – Ukrainian electrical grids are targeted by new malware. (Mike Rogers statement to SASC, 2-27-18)

February 27, 2018 – USCYBERCOM Commander Adm. Mike Rogers tells the Senate Armed Services Committee: “We are monitoring the cyber conflict sparked by the ongoing Russian-manufactured conflict in Ukraine. Secretary Mattis in Kyiv noted that Russia is not adhering to the letter or the spirit of its treaty commitments, most egregiously by attempting to change international borders by force. This behavior in geographic space matches Russian cyberspace behavior; Russia’s cyber actions seem designed to complement and support its aggressive actions on the ground. While we cannot discuss the details in open session, I would draw your attention to the spate of very serious cyber attacks against Ukrainian citizens and infrastructure over the last 16 months.” (Mike Rogers statement to SASC, 2-27-18)

April 13, 2018 – A Russian court gives Roskomnadzor (Federal Service for Supervision of Communications, Information Technology and Mass Media), Russia’s communications oversight agency, the authority to ban the Telegram app for not providing a backdoor to allow government decryption and surveillance of messages. The platform has 200 million users worldwide. The company insists the app has nothing like a master-key to decrypt its communications. ([Russia Bans Telegram, China's Facial Recognition, and More Security News This Week | WIRED](#))

Subsequent news accounts indicate the banning effort is a bust, at least as far as its primary target. Telegram succeeds in evading Roskomnadzor’s blocking attempts mainly through “domain fronting” – disguising the source of its traffic by having its services hosted on another organization’s (Google and Amazon) web services. (Coincidentally or not, Google soon announces it will be disabling domain fronting, calling it a “quirk” that was never supposed to exist. The move is met with calls to keep the option available for the sake of human rights and internet freedom principles.) Unfortunately, while Telegram has escaped censorship, a side effect is that many other sites including Twitter, Facebook, Google, Yandex, and VKontakte still face partial or temporary blocks. ([This is why Russia's attempts to block Telegram have failed | WIRED UK](#))

*Wired* quotes Censored Planet’s Leonid Evdokimov as saying this is having a chilling effect because it shows the government has little or no concern about collateral damage. “Thousands of low-profile websites are still blocked because of that incident. So it's complicated ... I would not say that I'm full of optimism, but I see that people learn how to circumvent internet censorship really quickly when they want to. But they have to want to.” ([Russia Takes a Big Step Toward Internet Isolation | WIRED](#))

*Wired* writer Matt Burgess makes the point that the Telegram experience shows that there are still real limits to access and free information flows in the digital age. “Despite the global nature of the web, the internet still requires physical infrastructure to operate. Physical cables and servers are controlled within the borders of nations and fall under the laws of those states.” ([This is why Russia's attempts to block Telegram have failed | WIRED UK](#))

Roskomnadzor finally lifts the ban on June 18, 2020 (see entry below).

April 25, 2018 – Less than two weeks after a Russian court authorizes the banning of Telegram, the Russian Education Ministry’s Science Council reports that Roskomnadzor’s blocking attempts have inadvertently cut off access to online scholarly resources that are “extremely important for scientific work.” The Council calls the impact “serious.” “The disruption of scientific work throughout the country is too high a price to pay for a clumsy attempt to enforce a court ruling against a single company.” ([A scientific council says the Telegram ban is causing ‘serious damage’ to Russia's scientific research capacity — Meduza](#))

October 4-17, 2018 – Russian “law enforcement authorities” restrict access to social media in the troubled Ingushetia region by instructing two mobile operators to shut down most access to affected data services. While 3G and 4G services were targeted, 2G services were still operating, allowing users to make voice calls. It is reportedly the first documented case of such a crackdown. It follows an outbreak of protests over the drawing of Ingushetia’s border with Chechnya. ([Russia stifled mobile network during protests: document | Reuters](#))

November 6, 2018 – U.S. midterm congressional elections take place. According to a later media report citing several U.S. officials, USCYBERCOM over several days during this period covertly blocks web access to the Internet Research Agency, the St. Petersburg-based company believed to be responsible for significant meddling in U.S. electoral politics. The *Washington Post* reports: “The operation marked the first muscle-flexing by U.S. Cyber Command, with intelligence from the National Security Agency, under new authorities it was granted by President Trump and Congress last year to bolster offensive capabilities. The president approved of the general operation to prevent Russian interference in the midterms, officials said.” Cyber expert Herbert Lin later suggests the operation may have provided a precedent for U.S. strategy in the war in Ukraine. ([U.S. Cyber Command operation disrupted Internet access of Russian troll factory on day of 2018 midterms - The Washington Post](#); [Lin-Russian Cyber Operations in Ukraine-Cyber Defense Review-2022-fall.pdf](#))

2019 – Around this time, a rift becomes evident between Russian hackers and cyber criminals from elsewhere in the former Soviet space, according to reports later. Whereas post-Soviet hackers used to collaborate regularly in crime, one observer notes, 2019 witnessed a widening split especially between Russians and Ukrainians along with “a growing unease that Ukraine was co-operating with Western cyber-police, which itself was a consequence of Western countries providing aid to

strengthen Ukraine's cyber-defenses." (András Tóth-Czifra of the D.C.-based Flashpoint Intelligence, quoted by al Jazeera in 2022.) ([Russia-Ukraine war reaches dark side of the internet | Russia-Ukraine war News | Al Jazeera](#))

Mid-2019 – According to the U.S. government and the U.K.'s NCSC, around this time, the GRU begins conducting "brute force access attempts" against government and private sector organizations in an effort to acquire sensitive information. (Russian GRU Conducting Global Brute Force Campaign to Compromise Enterprise and Cloud Environments – NSA)

July 27 & August 3, 2019 – Russian authorities institute a "targeted internet shutdown" during street demonstrations in Moscow. Internet measurements of Russia's IP space by Netblocks show that between 12:00 p.m. UTC and 2:30 p.m. the state-run Rostelecom network AS12389 "experienced a small, but detectable, anomalous fall in connectivity consistent with a targeted localised internet shutdown that is understood to have affected fixed-line and wifi connections." The BBC later quotes a letter to staff at an unidentified Russian telecom company it obtained that indicates parts of base stations were "disconnected at the request of law enforcement agencies." "Purposeful or politically motivated Internet shutdowns are rare in Moscow," Netblocks writes. ([Evidence of internet disruptions in Russia during Moscow opposition protests - NetBlocks](#); [Internet during rallies in Moscow could be jammed at the request of security forces - BBC News Russian service](#))

October 21, 2019 – The hacktivist threat group Joker DPR sets up its first Telegram channel. ([Joker DPR and the Information War \(recordedfuture.com\)](#))

November 1, 2019 – The law on the "sovereign Runet" enters into force in Russia. According to *Vedomosti*: "It obliges telecom operators to install equipment on their networks, which will be provided to them by Roskomnadzor [the government's communications oversight agency], in order to centrally manage the routing of traffic in the event of a threat to the Runet. The same equipment will allow the department to filter traffic and block access to resources from the list of prohibited in Russia." ([Минкомсвязи подвело итоги первых учений по закону о «суверенном рунете» - Ведомости \(vedomosti.ru\)](#))

November 27, 2019 – An article in TechCrunch highlights certain difficulties Western companies sometimes face in situations like the Russian seizure of Crimea. As an example, Apple and Google Maps have both felt compelled to partially accommodate Moscow's demands that the annexed territory be displayed as part of Russia for viewers from there – a requirement of "Russian legislation," according to government officials. ([Apple and Google Maps accommodate Russia's annexation of Crimea | TechCrunch](#))

December 16-17, 2019 – The Ministry of Communications runs its first tests of the new (as of November 1) law on the "sovereign Internet." Deputy Minister Alexei Sokolov, who led the exercises, tells journalists they took place over several days in Moscow,



Vladimir, Rostov and in several other regions. Four telecom operators – Rostelecom, VimpelCom, MTS, MegaFon – take part, along with the Ministry of Internal Affairs, the Ministry of Defense, the Ministry of Energy, the Federal Security Service, Rosgvardia, Kaspersky Lab, Positive Technologies and Group-IB. The following were tested: stability of communications, security of cellular communications, including the protection of personal data and traffic interception, and the security of the “Internet of Things.”

For each of the four commercial operators, according to the Russian outlet *Vedomosti*, “18 attack scenarios were worked out – 12 through the signal networks of the SS7 protocol (the channel through which service commands are transmitted to connect subscribers in telephone networks around the world) and six through the signal networks of the Diameter protocol (one of the main protocols in 4G networks). Each scenario took about 20 minutes to work out.” “According to the presentation, a simulated attacker managed to successfully carry out 62.5% of attacks through the SS7 protocol and 50% of attacks through the Diameter protocol. The detection time for each attack averaged 2-3 minutes.”

According to Sokolov, “in general, the authorities and telecom operators” are now prepared to confront an external threat. Exercises are to take place at least once a year. ([Минкомсвязи подвело итоги первых учений по закону о «суверенном рунете» - Ведомости \(vedomosti.ru\)](#))

*Wired* quotes Mikhail Klimarev, executive director of the Internet Protection Society, a Russian NGO, as saying the tests are mostly for propaganda and to raise alarms about the government's technical capabilities. “About the military exercises of the ‘sovereign internet’ I can only say that this is fraud,” Klimarev insists. “On the orders of the government they really can turn off the internet in some places—we have already observed two such cases. But technically it's very difficult to make a shutdown in Russia. There are roughly 3,500 telecom operators in Russia.” ([Russia Takes a Big Step Toward Internet Isolation | WIRED](#))

2020-2022 – In May 2023, Malwarebytes publishes a report on a newly-identified APT actor they refer to as “RedStinger.” While, according to the report, the group is likely Russian, they curiously seem to have been focusing on both Ukrainian and Russian targets; thus the group cannot be attributed to a specific country. The group’s goals of surveillance and data gathering were not carried out in the most sophisticated fashion, according to Malwarebytes; however, Kaspersky researchers later release a report on the same group claiming that they have been active as far back as 2008, making their anonymity and quiet offensive cyber campaigns more notable. ([Uncovering RedStinger - Undetected APT cyber operations in Eastern Europe since 2020](#) – Malwarebytes; [CloudWizard APT: the bad magic story goes on](#) – Kaspersky)

2020-2022 – Speaking at a cyber conference in June 2022, Neal Higgins, deputy national cyber director for national cybersecurity, comments that “The last 24 months have seen an unprecedented surge in high-profile cyber events, from SolarWinds beginning in late 2020, through Kaseya, Colonial Pipeline, JBS Foods, and now the use of cyberattacks in connection with the ongoing Russian invasion of Ukraine.”

(Speaking at Defense One, June 14, 2022, [Prolonged war may make Russia more cyber aggressive, US official says \(yahoo.com\)](#))

May 2020 – “Beginning in 2020, USAID launched an ambitious \$38 million cybersecurity reform program, according to a later State Department release. The program “will work over the next several years to strengthen Ukraine’s cybersecurity legal and regulatory environment, build Ukraine’s cyber workforce and strengthen course offerings at leading Ukrainian universities, and develop connections between critical infrastructure operators and private sector solution providers. This program has embedded more than 20 technical experts within the Government of Ukraine to bolster Ukraine’s cyber response and recovery capabilities, and deployed cybersecurity software and hardware tools to ensure the resilience of critical infrastructure to physical and cyber attacks.” ([U.S. Support for Connectivity and Cybersecurity in Ukraine - United States Department of State](#))

A separate USAID fact sheet in 2022 added these details: “USAID launched the four-year, \$38 million Cybersecurity for Critical Infrastructure in Ukraine activity in May 2020 and to strengthen Ukraine’s cyber preparedness and protect critical infrastructure through assistance in three key directions: 1) strengthening the cybersecurity enabling environment; 2) developing Ukraine’s cybersecurity workforce; and 3) building a resilient cybersecurity industry.” The release contains further information. ([Cybersecurity Fact Sheet | Ukraine | U.S. Agency for International Development \(usaid.gov\)](#))

June 18, 2020 – Roskomnadzor finally lifts its ban on Telegram “in agreement with Russia’s general prosecutor’s office.” The injunction was basically a failure and some government officials and departments were known to use the platform and even maintain official channels on it. Roskomnadzor, however, declares that the reason for reversing the ban is that the app’s found, Pavel Durov, has said he will cooperate in the fight against terrorism and extremism. ([Russia lifts ban on Telegram messaging app after failing to block it | Reuters](#))

August 2020 – The Belarusian Cyber Partisans form following the disputed re-election of Alexander Lukashenko. Starting as a small collection of tech specialists who have to train themselves in hacking, the Partisans grow into a significant opposition group whose members the government considers terrorists. ([How Belarusian hacktivists are using digital tools to fight back - The Record by Recorded Future](#))

2021

2021

2021

2021

2021

2021 – Over the course of the year, APT28, believed by Western intelligence agencies to be the GRU’s 85th special Service Centre (GTsSS) Military Intelligence Unit 26165, exploits vulnerabilities in Cisco routers around the world, including roughly 250 Ukrainian targets, using the routers to conduct reconnaissance and deploy malware. ([APT28 exploits known vulnerability to carry out... - NCSC.GOV.UK](#))

January 2021, 2022 – Iran and Russia sign an agreement on cybersecurity cooperation.  
([After Ukraine: Russia's Potential Military and Nuclear Compensation to Iran | The Washington Institute](#))

January 2021 – October 2021 – Ukraine is “the victim of roughly 288,000 cyberattacks in the first 10 months of 2021,” according to *Politico*, citing Ukrainian government official estimates. “(As a comparison, traditional munitions were exchanged an average of 67 times each day in the Donbas region last year, according to the OSCE.) It’s unclear whether the attacks originate from the Kremlin, or Russian-backed hacker syndicates, or elsewhere, though many attacks have been attributed to Russia.” ([‘Kill Your Commanding Officer’: On the Front Lines of Putin’s Digital War With Ukraine - POLITICO](#))

February 2021 – July 2022 – In a later interview with *Politico*, Yurri Shchychol, head of the State Service of Special Communications and Information Protection, describes his country’s attempts to anticipate Russian cyberattacks starting well over a year before the invasion: “Of course, we were preparing ourselves for this, and in the last 18 months [as of July 2022] most of our preparations in advance were to be able to withstand widespread attacks against multiple targets. We ensured uninterrupted exchange of information between all [government and civil organizations], sharing information regarding the criteria for compromising networks. We also worked on building up the technical capabilities of government institutions so they could quickly gather server data, make copies, and share those copies with us [ahead of a Russian attack].”

Shchychol adds: “In all those efforts we had very strong support from our private sector. It’s worth mentioning that a lot of private sector IT cybersecurity experts are either directly serving in the Armed Forces of Ukraine or my State Service or otherwise are indirectly involved in fighting against cyberattacks, and those private sector assistants of ours are world class experts who used to work in leading global companies taking care of their cybersecurity.” ([The Man at the Center of the New Cyber World War - POLITICO](#))

February 2021 – Ukraine’s Security Service is hit by a multi-day DDoS attack. (Rob Joyce at RSAC 2022)

March 2021 – As early as this month, Russia-aligned groups may have been pre-positioning for a conflict, according to a Microsoft report. ([An overview of Russia’s cyberattack activity in Ukraine \(microsoft.com\)](#))

March 2021 – Ukraine fends off a Russian attempt to hack its classified military systems. (Rob Joyce at RSAC 2022)

Early 2021 – “Russian actor NOBELIUM launched a large-scale phishing campaign against Ukrainian interests involved in rallying international support against Russian actions,” according to a later Microsoft report. “Similarly, DEV-0257 (publicly

known as Ghostwriter) began phishing campaigns attempting to gain access to Ukrainian military email accounts and networks.” ([An overview of Russia’s cyberattack activity in Ukraine \(microsoft.com\)](#))

April 15, 2021 – U.S. cyber agencies – the NSA, CISA, and FBI – publicly link Cozy Bear (also known as APT29, and The Dukes) directly with Russia’s Foreign Intelligence Service (SVR). ([CSA SVR TARGETS US ALLIES UOO13234021.PDF \(defense.gov\)](#))

May 28, 2021 – Twenty-three countries affirm their adherence to principles of “responsible state behavior” in the cyber sphere. The process took place pursuant to U.N. General Assembly resolution 73/266 and builds on the work of the United Nations Groups of Governmental Experts (GGEs). (“Report of the Group of Governmental Experts on Advancing responsible State behaviour in cyberspace in the context of international security,” 5-28-21)

June 16, 2021 – Presidents Biden and Putin meet in Geneva. Biden tells reporters he warned Putin the U.S. would resort to offensive cyber operations if the Russians did not pull back on hits against American targets. But he adds that he told the Russian leader that some 16 critical infrastructure sectors should be ruled out as targets. ([Biden says he told Putin U.S. will hack back against future Russian cyberattacks - POLITICO](#))

The White House indicates that Biden and Putin spoke by telephone today, the subject being about “ongoing ransomware attacks by criminals based in Russia that have impacted the United States and other countries,” according to a White House readout. “President Biden reiterated that the United States will take any necessary action to defend its people and its critical infrastructure in the face of this continuing challenge.” ([Readout of President Joseph R. Biden, Jr. Call with President Vladimir Putin of Russia - The White House](#))

Mid-2021 – Ukraine opens the UA30 Cyber Center training facility for the private sector. Ukrainian information security official Yurri Shchyhol tells *Politico* in July 2022: “This training center of ours launched into operation more than one year ago and over that period of time we conducted more than 100 training sessions for civilian contractors, private sector, military operators, all focused on cybersecurity. We conducted a number of hackathons and competitions. Even though we conducted a few training sessions after the beginning of the renewed conflict, the location of the training center is not safe. So we’re not using it that much right now.

“This center was aimed to deepen the knowledge-sharing between the private sector and the government, those tasked with overseeing information protection across various government bodies and institutions. It’s a hub that fosters the knowledge of the private sector. We treat it as a competence center that allows all the industries and sectors involved to grow by helping each other.” ([The Man at the Center of the New Cyber World War - POLITICO](#))

Mid-2021 – By this point, Microsoft is observing “known and suspected Russian threat actors separately targeting supply chain vendors in Ukraine and abroad to secure



accesses and pre-position for future third-party intrusions against Ukraine and its partners in NATO. DEV-0586, a previously unknown group with suspected Russian military ties, had compromised the network of an IT firm that built resource management systems for Ukraine's Ministry of Defense and organizations in the communications and transportation sectors." ([An overview of Russia's cyberattack activity in Ukraine \(microsoft.com\)](#))

Mid-2021 – In this period, according to Microsoft later, the Russian threat actor "NOBELIUM attempted to access IT firms serving government customers in predominantly NATO member states, at times successfully compromising then leveraging privileged accounts to breach and steal data from Western foreign policy organizations ... Roughly 93% of all Russia-backed attack activity observed in our online services was aimed at NATO member states, particularly against the United States, the United Kingdom, Norway, Germany, and Turkey through 2021." ([An overview of Russia's cyberattack activity in Ukraine \(microsoft.com\)](#))

July 2021 – A Russia-linked group called Shuckworm (Gamaredon, Armageddon) attacks Ukrainian systems, part of a long campaign targeting the country since 2014. "While the group's tools and tactics are simple and sometimes crude," according to Symantec's Threat Hunter Team, "the frequency and persistence of its attacks mean that it remains one of the key cyber threats facing organizations in the region." Symantec has found four variants of Pterodo malware in the recent attacks. ([Battling Moscow's hackers prior to invasion gave Kyiv 'full dress rehearsal' for today's cyber warfare \(cyberscoop.com\)](#); [\(1\) New Messages! \(security.com\)](#))

July 1, 2021 – The NSA, CISA, FBI and the U.K.'s NCSC release a joint Cybersecurity Advisory exposing malicious activity by the GRU against "hundreds of government and private sector targets worldwide." The report details how, since mid-2019 and likely still ongoing, the GRU has purportedly been conducting widespread "brute force access attempts" targeting sensitive information. (Russian GRU Conducting Global Brute Force Campaign to Compromise Enterprise and Cloud Environments – NSA)

July 27, 2021 – President Biden mentions the prospects of a "shooting war" resulting from a future cybersecurity incident. "You know, we've seen how cyber threats, including ransomware attacks, increasingly are able to cause damage and disruption to the real world. I can't guarantee this, and you're as informed as I am, but I think it's more likely we're going to end up — well, if we end up in a war, a real shooting war with a major power, it's going to be as a consequence of a cyber breach of great consequence. And it's increasing exponentially — the capabilities." (Remarks by President Biden, 7-27-21)

August 2021 – As Microsoft reports later, Russian actor "ACTINIUM launched spear-phishing campaigns to gain access to accounts of Ukraine-based foreign military advisors and humanitarian workers, in August. Around the same time, STRONTIUM attempted to compromise defense-related organizations in Ukraine. ACTINIUM,

NOBELIUM, BROMINE, SEABORGIUM, and DEV-0257 sought persistent access to their particular interests among a total target pool that included Ukrainian defense, defense industrial base, foreign policy, national and local administration, law enforcement, and humanitarian organizations.” ([An overview of Russia’s cyberattack activity in Ukraine \(microsoft.com\)](#))

August 31, 2021 – U.S. and Ukrainian defense ministers sign the “U.S.-Ukraine Strategic Defense Framework,” which includes a provision for “Strengthening cooperation on cyber security to deter malicious cyber activities on national security systems, to attribute such activities, and to defend against adversaries effectively.” (Document, 8-31-2021)

No date – According to remarks in late 2022 by Iran’s foreign minister, Hossein Amirabdollahian, the Islamic Republic delivered an unspecified number of drones “months before” its February 24, 2022, invasion of Ukraine. When Western officials report later that Russia has used Iranian drones, notably against civilians, Iran denies providing the weapons specifically for use in the war. Western officials further report, however, that Iran has sent trainers to Russian-occupied parts of Ukraine to help with problems with the drones. ([Drone delivery dates back to months before Ukraine war: Iran FM - IRNA English](#); [Iran Acknowledges Sending Drones to Russia, but Says This Preceded War - The New York Times \(nytimes.com\)](#))

October 11, 2021 – In a later interview with *Politico*, Gen. Paul Nakasone recalls: “By the 11th of October, I’m convinced the Russians are going to invade Ukraine. The preponderance of intelligence was different than anything we’d ever seen before.” ([‘Something Was Badly Wrong’: When Washington Realized Russia Was Actually Invading Ukraine - POLITICO](#))

Fall 2021 – In a later interview, Anne Neuberger, deputy national security adviser for cyber and emerging technology, tells *Politico*: “This was really a coming-of-age for our cyber community — we never before mobilized like this for a geopolitical crisis. It reflects the extent to which cyber was now a mainstream national security issue. The White House had three major lines of effort [on the cyber side]: We mobilized to provide a range of assistance to the Ukrainians, we mobilized with the international community, and we really mobilized across the U.S. government and the private sector in a way we never did before.” ([‘Something Was Badly Wrong’: When Washington Realized Russia Was Actually Invading Ukraine - POLITICO](#))

November 18, 2021 – Secretary of Defense Lloyd Austin meets with Ukrainian Defense Minister Oleksii Reznikov at the Pentagon. Austin says he looks forward to discussing ways to “counter Russian aggression and to deepen our cooperation in such areas as Black Sea security, cyber defense and intelligence sharing.” ([Austin: U.S. Will Work With Ukraine, Allies to Counter Russian Aggression > U.S. Department of Defense > Defense Department News](#))

November 19, 2021 – The day after his “last-minute” visit with Secretary of Defense Austin, Ukrainian Defense Minister Reznikov holds a press conference which includes remarks about post-2014 U.S. assistance to Ukraine that has averaged more than \$200 million a year. Among a slew of military hardware he mentions high-tech communications equipment the U.S. provided after Russia intercepted Ukrainian military communications. ([Ukraine Requests New Defense Assistance Amid Increased Tensions With Russia - Air Force Magazine](#))

November-December 2021 – Anne Neuberger tells an interviewer later that in this period “We were absolutely concerned because Russia has a history with Ukraine — as well as with Georgia and Estonia — in terms of using cyber in a destructive way as part of a geopolitical situation. We’re very concerned, based on the history, that they would disrupt Ukrainian power, but also really use cyber to destabilize and demoralize, to convey to the Ukrainian population, “Your government is not functional.”

Also in this timeframe, “We brought the Ukrainian energy team here to work with our national labs. We shared a whole list of targets that the Russians had compromised to enable the Ukrainians to rapidly address them; we put a real focus on their energy systems, and the Cyber Command team focused on military and transportation networks.”

([‘Something Was Badly Wrong’: When Washington Realized Russia Was Actually Invading Ukraine - POLITICO](#))

November-December 2021 – Speaking to a reporter later about the Biden administration’s decision to release sensitive information about Russia’s plans and actions to the public, NSC Spokesperson Emily Horne says: “Taking a step back, the information environment had changed dramatically since 2014. One, there’s a ton of commercially available satellite imagery, open source, and anyone with access to those images could see for themselves what Russia was doing on Ukraine’s borders. Second, there had been just an explosion in citizen journalism in the use of social media to show in real time what people were actually seeing, and this is coming from both Russian and Ukrainian sources. It was out there on Twitter, it was out there on TikTok. People could see for themselves, what these troops were doing — in some cases where they were. Then third, you have a general public that has a fundamentally different understanding of disinformation and misinformation — those terms are in people’s vocabularies in a way that they weren’t in 2014.”

([‘Something Was Badly Wrong’: When Washington Realized Russia Was Actually Invading Ukraine - POLITICO](#))

Late 2021 – Late in the year, according to a subsequent Microsoft report, “suspected Russian cyber actors positioned themselves in networks of Ukrainian energy and IT providers that were later targets of destructive attacks, including Kitsoft, the IT service provider that DEV-0586 compromised to facilitate destruction on the networks of several clients in January 2022.” ([An overview of Russia’s cyberattack activity in Ukraine \(microsoft.com\)](#))

December 2021 – CISA’s Joint Cyber Defense Collaborative (JCDC) becomes involved in supporting Ukraine. Eric Goldstein, CISA Executive Assistant Director for Cybersecurity, later testifies to a House Homeland Security subcommittee: “We are also deeply focused on the JCDC as a locus of proactive planning. Looking briefly at our work around the Russian invasion of Ukraine, in December [2021], we developed a joint public-private cyber defense plan.” (See also January 2022 entry) ([Congressional Document \(wrlc.org\)](#))

According to CrowdStrike Senior VP Adam Meyers in April 2022: “The US government has made significant strides over the past several years in coordinating with industry against cyber threats. The establishment of JCDC in particular, where CrowdStrike participates as a plank holder, has helped strengthen industry and government collaboration.” (House Homeland Security Subcommittee on Cybersecurity, Infrastructure Protection and Innovation, hearing on Russian cyber threats, 4-5-22)

December 2021 – Roskomnadzor, acting on a 2017 court order, orders internet service providers (ISPs) to block the Tor Project website and restrict access to its services. “Since then, censors have been locked in a battle with Tor’s technical team and users in Russia,” *Wired* reports later. One approach Tor uses is volunteer-run “bridges” that serve as entry points whose details are not public and are therefore hard to disrupt. ([How Tor Is Fighting—and Beating—Russian Censorship | WIRED](#))

December 2021 – Ukraine resorts to a variety of sources for help in fending off attempted cyber hits, including Western news accounts. Speaking a year later to the *Washington Post*, Mykhailo Fedorov, vice prime minister and minister of digital information, says: “We ended up getting a lot of information about cyberattack vectors and other related information from the media. And that is how we were able to prevent attacks on our energy infrastructure back in December [2021].” ([Ukraine gets by in cyberspace with a little help from its friends - The Washington Post](#))

December 2, 2021 – (See also December 4, 2021, entry below) A U.S. military team travels to Ukraine led by a Marine Corps major, Gen. Paul Nakasone says later. “[H]er guidance was this: Go help them, and make sure they’re ready, in terms of anything that may occur.” (This is presumably the same team mentioned in the December 3 entry below.) ([Advance work in Ukraine blunted Russian cyber advantage, US says \(c4isrnet.com\)](#))

Further describing hunt forward operations, Nakasone adds: “You know, having ten folks on the ground that are tied back to our command and our agency, that’s a power that I think is really helpful .... [It] begins with ten, and then we surged to well over thirty. And so we had flooded the zone. And in terms of—just to kind of give you a metric, you know, since 2018 we have done thirty-seven operations, twenty nations, on fifty-five different networks. This is, you know, an opportunity for us to help our partners. It’s also a way that we think about how do we secure the United States and how do we look at the malware that we see? Because every time we see it and then we share it with industry, we inoculate all of that badness that comes with those actors doing that type of work.” ([Cyber](#)



[Collaboration in the Age of Hybrid Warfare: A Conversation With Jen Easterly and Paul Nakasone | Council on Foreign Relations \(cfr.org\)](#)

According to a November 2022 press release, “In addition to conducting a hunt forward on the ground, the team provided remote analytic and advisory support using new and innovative techniques, and conducted network defense activities aligned to critical networks.” ([Before the Invasion: Hunt Forward Operations in Ukraine > U.S. Cyber Command > News](#))

December 3, 2021 – (See also December 2 entry above) *Air Force Magazine* reports: “A Defense Department team is on the ground in Ukraine assessing what the country needs to protect itself from air, naval, electronic, and cyber warfare threats as Russian troops gather on multiple fronts, a senior Ukrainian defense official told *Air Force Magazine*, describing an emphasis on what assistance can be delivered ‘today’.” The visit follows a request by Defense Minister Reznikov during his November 18 meeting with Secretary of Defense Austin at the Pentagon. ([With Russia on Multiple Fronts, DOD Team in Ukraine Assesses Air Defense Needs - Air Force Magazine](#))

December 3, 2021 – The U.S. Intelligence Community releases an unclassified, unattributed 1-page document displaying satellite photos (from DigitalGlobe) and a map showing the disposition of Russian forces around Ukraine. The lengthy title is: “Potential for 175,000 Russian Forces Near Ukraine: Evidence of Recent Artillery, Equipment, Personnel Movements and Planning.” It is the result of a decision reportedly by President Biden personally to aggressively expose and thereby undermine Russian plans and operations by declassifying intelligence at a level observers say is unprecedented. Emily Horne says later this is the first time the administration put this idea into practice. ([Russia planning massive military offensive against Ukraine involving 175,000 troops, U.S. intelligence warns - The Washington Post](#); [Ukraine: Inside the spies’ attempts to stop the war - BBC News](#); [‘Something Was Badly Wrong’: When Washington Realized Russia Was Actually Invading Ukraine - POLITICO](#))

December 4, 2021 – (See also December 2, 2021, entries above) According to Gen. Paul Nakasone in a later interview with *Politico*, “We sent a [U.S. Cyber Command] team forward, and they land in Kyiv on the fourth of December. Within a day or two, the leader calls back, and she tells my Cyber National Mission Force commander, her boss, “We’re not coming home for a while. In fact, send more people.” We sent our largest “hunt forward” package into Kyiv. That stays there for a little over 70 days. What is a “hunt forward” operation? A hunt forward operation is focused at the partner’s request to look at a series of networks — we identify malware, tradecraft and anomalous behavior in those networks that point us to adversaries and allow the partner — in this case, Ukraine — to strengthen those networks.

“The interesting thing that she — the team leader — said: ‘They’re really serious about this.’ This is the third time that we had been back in Ukraine, and there was just a different feeling in terms of how Ukraine was approaching it. When we provided information, they were moving on it, correcting the vulnerability, and

looking for more.” ([‘Something Was Badly Wrong’: When Washington Realized Russia Was Actually Invading Ukraine - POLITICO](#))

December 6, 2021 – A New Jersey Superior Court Judge rules that an insurance company’s denial of coverage to Merck & Co. for losses sustained as a result of the 2017 NotPetya attack was invalid. Ace American Insurance Company had cited an “act of war” exclusion to deny Merck’s claim, but the judge’s order determines that the war exclusion only applies to armed conflict and that insurers should have put their customers “on notice” that cyberattacks would not be covered. (Superior Court of New Jersey, Docket No.: U.N.-L-2682-18, 12-6-21; [Merck’s \\$1.4 Billion Insurance Win Splits Cyber From ‘Act of War’ \(bloomberglaw.com\)](#))

December 8, 2021 – The RAND Blog publishes a commentary that posits: “If Russia were to invade Ukraine, it would likely employ massive cyber and electronic warfare tools and long-range PGMs. The aim would be to create ‘shock and awe,’ causing Ukraine’s defenses or will to fight to collapse. This was wishful Soviet thinking early in its Afghanistan war and America’s calculus early in the Iraq war.” ([If Russia Invaded Ukraine | RAND](#))

December 15, 2021 – The EU approves a €31 million assistance package for Ukraine’s Armed Forces under the European Peace Facility that includes support for cyber defense. Part of the funding will go toward the Communication and Cyber Security Command of Ukraine and feature a cyber-lab and security software and hardware. The latter elements are finally delivered almost a year later. ([Ukraine: EU sets up a cyber lab for the Ukrainian Armed Forces | EEAS Website \(europa.eu\)](#))

December 20, 2021 – The *New York Times* reports that “the United States and Britain have quietly dispatched cyberwarfare experts to Ukraine in hopes of better preparing the country to confront what they think may be the next move by President Vladimir V. Putin of Russia as he again menaces the former Soviet republic: Not an invasion with the 175,000 troops he is massing on the border, but cyberattacks that take down the electric grid, the banking system, and other critical components of Ukraine’s economy and government.” Few details are available. ([U.S. and Britain Help Ukraine Prepare for Potential Russian Cyberassault - The New York Times \(nytimes.com\)](#))

December 20, 2021 – The *New York Times* quotes Sen. Angus King (I-ME): “I don’t think there’s a slightest doubt that if there is an invasion or other kind of incursion into Ukraine, it will start with cyber.” King is one of the leaders of the government’s Cyberspace Solarium Commission. The other commission leader, Rep. Mike Gallagher (R-WI) advocates for a firm response if Russia acts first: “We have very powerful weapons in the cyberdomain that we could use against Putin if he chooses to go further. We seem divided, but there’s a lot of options we have to prevent this from devolving into a full-on crisis.” ([U.S. and Britain Help Ukraine Prepare for Potential Russian Cyberassault - The New York Times \(nytimes.com\)](#))

December 23, 2021 – Russian hacking group UAC-0056 makes its first known breach of Ukrainian government servers, according to CERT-UA much later. ([Detected cyberattack on a number of Ukrainian government information resources \(cip.gov.ua\)](#); [Ukraine says Russian hackers backdoored govt websites in 2021 \(bleepingcomputer.com\)](#); Risky Biz News, 2-26-2023)

Late December 2021 – According to a later account from the American Water Works Association: “In late December, working with our sector partners EPA and CISA, we reached out through EPA to 58,000 water systems, alerting them to Russian cyber-threat activities identified by CISA. The associated advisories have been shared across multiple communication platforms to ensure the widest possible distribution.” (House Homeland Security Subcommittee on Cybersecurity, Infrastructure Protection and Innovation, hearing on Russian cyber threats, 4-5-22)

December 2021 – January 2022 – USCYBERCOM and Ukraine’s Cyber Command conduct a series of defensive cyber operations, according to a later State Department release. The cooperation is “part of a wider effort to increase cyber resilience in critical networks. Cyber professionals from both countries sat side by side, looking for adversary activity and identifying vulnerabilities. In addition to this effort, the team provided remote analytic and advisory support aligned to critical networks from outside Ukraine.” ([U.S. Support for Connectivity and Cybersecurity in Ukraine - United States Department of State](#))

USCYBERCOM Commander Nakasone comments later: “We went in December 2021 at the invitation of the Kyiv government to come and hunt with them. We stayed there for a period of almost 90 days.” ([US military hackers conducting offensive operations in support of Ukraine, says head of Cyber Command | Science & Tech News | Sky News](#))

2022

2022

2022

2022

2022

January 2022 – CISA’s Joint Cyber Defense Collaborative (JCDC) runs exercises for a joint public-private cyber defense plan developed the previous month (see entry). Eric Goldstein of CISA testifies later to a congressional subcommittee: “We exercised this plan in January, and when the invasion occurred, we moved into execution...” ([Congressional Document \(wrlc.org\)](#))

January 2022 – Russian actor DEV-0586 compromises IT service provider Kitsoft in order to “facilitate destruction on the networks of several clients,” according to Microsoft. ([An overview of Russia’s cyberattack activity in Ukraine \(microsoft.com\)](#))

January 2022 – Disinformation scholar Adéla Klečková publishes a lengthy report on “The Role of Cyber ‘Elves’ Against Russian Information Operations” for the German Marshall Fund. The elves are a “group of cyber activists fighting pro-Kremlin propaganda and disinformation campaigns.” They are “growing yet little-known

phenomenon. Having started in 2014 as less than 20 individuals in Lithuania, the movement expanded to 13 Central and East European countries, and it counted about 4,000 volunteers by 2021.” The loosely tied group will come to play an increasing role after the February Russian invasion of Ukraine. “[I]t would be unwise to overlook or underestimate this movement,” the author writes. ([Kleckova - Elves cyber activism - paper - DocumentCloud](#))

January 2022 – In an interview with *Politico*, Gen. Paul Nakasone says: “In January, the National Security Agency is releasing cybersecurity advisories at an unclassified level to alert what we are seeing from our partners in Ukraine, and also provide further information to what we might anticipate in the United States. This is one of the things that I’m thinking about all the time is, you know, “What are our vulnerabilities?” Working across the FBI, CISA and the Department of Homeland Security — what are we seeing that might inform us of what an adversary, in this case the Russians, might do to us? This was really active. These were conversations going on every day.” ([‘Something Was Badly Wrong’: When Washington Realized Russia Was Actually Invading Ukraine - POLITICO](#))

January 11, 2022 – CISA, NSA, and the FBI issue a joint Cybersecurity Advisory (CSA) providing an “overview of Russian state-sponsored cyber operations; commonly observed tactics, techniques, and procedures (TTPs); detection actions; incident response guidance; and mitigations. This overview is intended to help the cybersecurity community reduce the risk presented by these threats.” The CSA urges a “heightened state of awareness.” ([Understanding and Mitigating Russian State-Sponsored Cyber Threats to U.S. Critical Infrastructure | CISA](#))

January 12, 2022 – Contributing to the debate over Russia’s cyber plans for Ukraine, cyber expert Jason Healey writes in *War on the Rocks*: “If Russia does attack Ukraine in the coming weeks, the opening salvo is likely to be with offensive cyber capabilities.” ([Preparing for Inevitable Cyber Surprise - War on the Rocks](#))

January 13, 2022 – Microsoft identifies “intrusion activity originating from Ukraine that appear[s] to be possible Master Boot Records (MBR) Wiper activity.” Reporting later, the company writes: “During our investigation, we found a unique malware capability being used in intrusion attacks against multiple victim organizations in Ukraine.” ([Destructive malware targeting Ukrainian organizations - Microsoft Security Blog](#))

January 13, 2022 – National security adviser Jake Sullivan tells reporters: “Our intelligence community has developed information, which has now been downgraded, that Russia is laying the groundwork to have the option of fabricating the pretext for an invasion ... We saw this playbook in 2014. They are preparing this playbook again.” Reporting on a later example of U.S. officials warning about possible Russian actions, NBC noted: “It’s one of a string of examples of the Biden administration’s breaking with recent precedent by deploying declassified intelligence as part of an information war against Russia ... Coordinated by the White House National Security



Council, the unprecedented intelligence releases have been so frequent and voluminous, officials said, that intelligence agencies had to devote more staff members to work on the declassification process, scrubbing the information so it wouldn't betray sources and methods." ([First on CNN: US intelligence indicates Russia preparing operation to justify invasion of Ukraine | CNN Politics](#); [The U.S. is using declassified intel to fight an info war with Russia, even when the intel isn't rock solid \(nbcnews.com\)](#))

January 13-14, 2022 – On the same date that negotiations fail between Russia, the United States, Ukraine, NATO, and Europe, the GRU-affiliated DEV-0586 “deploys [the] WhisperGate wiper to [a] limited number of Ukrainian government and IT sector systems” defacing their websites. The attack disrupts 70 websites, severely damages six and defaces 22 others with the message: “Ukrainians! All information about you has become public ... Be afraid and expect worse.” The U.K.’s National Cyber Security Centre also concludes the GRU was “almost certainly involved.” CrowdStrike tracks the perpetrators as EMBER BEAR. ([Russia behind cyber attack with Europe-wide impact an hour... - NCSC.GOV.UK](#); Rob Joyce slide at RSAC 2022; [An overview of Russia's cyberattack activity in Ukraine \(microsoft.com\)](#); [SITREP Ukraine | Accenture](#); House Homeland Security Subcommittee on Cybersecurity, Infrastructure Protection and Innovation, hearing on Russian cyber threats, 4-5-22)

At least one expert advises against overstating the implications of these kinds of events. “Though an incident hitting several targets simultaneously may at first appear to be a complex, advanced operation, they could be the result of access to a single content management system [that maintains multiple websites],” according to John Hultquist, vice president of intelligence analysis at Mandiant. “It’s important not to overestimate the capability necessary to carry out this attack.” Hultquist adds are neither large-scale nor sophisticated. “A lightweight actor could do this.” Kim Zetter notes further that no data was destroyed notwithstanding a posted warning. Network administrators quickly took the affected sites offline for maintenance and investigation and “[b]y the end of the weekend nearly all sites had been restored.” ([What We Know and Don't Know about the Cyberattacks Against Ukraine - \(updated\) \(substack.com\)](#))

A year later, another cyber expert, Lukasz Olejnik, posts an analysis generally similar to Hultquist’s. He labels the event a “cyber-enabled information operation.” ([TechLetters Cyber Insights: Cyberoperation as a prelude to Ukraine 2022+ war, a year after \(substack.com\)](#))

January 13-14, 2022 – Further on the impact of this wiper attack, Ukrainian authorities “credit” it with helping to prepare the country for a major digital campaign against Russia. “For us it was like a full dress rehearsal,” Illya Vityuk, head of the cybersecurity department of the Ukrainian State Security Service, says later. He says Russia made a “mistake” with their timing because this and other recent breaches prompted the Ukrainians to concentrate on building up their digital defenses. “They could have waited for the beginning of the war and if it had happened it would have been a disaster,” said Victor Zhora, deputy head of Ukraine’s main cybersecurity agency, the State Service of Special Communications

and Information Protection. Instead they prematurely revealed some of Ukraine's vulnerabilities and made it easier for the country to rebound following the attacks that followed the initial invasion. ([Battling Moscow's hackers prior to invasion gave Kyiv 'full dress rehearsal' for today's cyber warfare \(cyberscoop.com\)](#); [Did Russia mess up its cyberwar with Ukraine before it even invaded? - The Washington Post](#))

January 14, 2022 – The head of Ukraine's State Service of Special Communications and Information Protection, Yurri Shchychol, later tells *Politico*: "In the early morning that day, I started talking to our European partners as well as our U.S. partners, their respective lines, ministries and government institutions, like CISA, and we started receiving and are still [mid-July 2022] receiving assistance from them on a daily basis."

Shchychol calls today's attacks by Russia the start of "the first cyber world war," noting that, beyond Ukraine, 5,000 wind turbines were hit in Germany. ([The Man at the Center of the New Cyber World War - POLITICO](#))

January 14-15, 2022 – Among Russia's cyber activities immediately preceding (and sometimes continuing after) the invasion are "attacks on public registers – databases storing citizens' and government data – to provide a base from which to launch future cyberattacks," according to a May 2022 report by Dmytro Dubov, head of Ukraine's International Centre for Defense and Security. (Dmytro Dubov, "Russia's in Ukraine: The War in Cyberspace" (Series No. 2)

January 14, 2022 – Serhiy Demedyuk, deputy secretary of Ukraine's National Security and Defense Council, tells Reuters that Ukraine believes the defacement of some 70 government websites was the work of a group known as UNC1151 and that it was meant to disguise more damaging activities. A media analysis points out that the incident poses a significant dilemma for the Biden administration – how to deal with other countries that may be acting on the Kremlin's behalf. ([Ukraine suspects group linked to Belarus intelligence over cyberattack | Reuters](#); [Suspected Belarus ties to Ukrainian hacks complicate Biden's quandary - POLITICO](#); [Ghostwriter-Report-Final.pdf \(cardiff.ac.uk\)](#))

January 14, 2022 – After repeated U.S. requests – and threats – Russia's FSB announces it has broken up the "organized crime gang" REvil. Few details are available. Two group members, Andre Bessonov and Roman Muromsky, are among those placed in custody. ([Ransomware Group REvil Dismantled in Raids, Russia Says - The New York Times \(nytimes.com\)](#); [Russia arrests REvil ransomware gang sought by U.S. - The Washington Post](#))

January 14, 2022 – This date "seems to mark the onset of the preparation phase of Russia's hybrid war," according to one media outlet later. (The CyberWire, Daily Briefing, 7-20-22)

January 15, 2022 – Serhiy Demedyuk, deputy secretary of Ukraine's national security and defense council, tells Reuters the recent defacements were "just a cover for more

destructive actions that were taking place behind the scenes and the consequences of which we will feel in the near future.” He does not provide details but identifies the hackers as the group UNC1151, or GhostWriter, which is tied to Belarus. ([What We Know and Don't Know about the Cyberattacks Against Ukraine - \(updated\) \(substack.com\)](#))

January 15, 2022 – The Microsoft Threat Intelligence Center (MTIC) reveals the discovery of WhisperGate malware on Ukrainian websites. (CISA, [Update: Destructive Malware Targeting Organizations in Ukraine | CISA](#); Rob Joyce slide at RSAC 2022)

January 15, 2022 on – Cisco reports later: “When both the website defacements and the first WhisperGate malware deployments occurred in mid-January, we were contacted by three Ukrainian government agencies we have worked with in the past. From that point on, we have continued to support the State Special Communications Service of Ukraine (SSSCIP), the Cyberpolice Department of the National Police of Ukraine and the National Coordination Center for Cybersecurity (NCCC at the NSDC of Ukraine). This support has largely taken the form of incident response, and we have turned the lessons learned in those responses into protections for all our customers.” ([Cisco stands on guard with our customers in Ukraine - Cisco Blogs](#))

January 16, 2022 – Ukraine blames Russia for attacks on Ukrainian websites. (Rob Joyce slide at RSAC 2022)

January 18, 2022 – Data wipes take place at Ukrainian government agencies. (Rob Joyce slide at RSAC 2022)

January 19, 2022 – Global Affairs Canada, the federal government entity responsible for the country’s diplomatic and global relations, is hit with a cyberattack that leaves some diplomats without access to certain online services. ([Cyber-Attack on Global Affairs Canada - Infosecurity Magazine \(infosecurity-magazine.com\)](#))

January 22, 2022 – The FSB takes steps to rein in the Infraud Organization, apparently in connection with U.S. requests. But Moscow says it has no plans to extradite members of the group to the U.S. ([Dark Covenant 2.0: Cybercrime, the Russian State, and the War in Ukraine \(recordedfuture.com\)](#))

January 22-23, 2022 – The pro-Russia hacktivist group Killnet registers online domains. ([Dark Covenant 2.0: Cybercrime, the Russian State, and the War in Ukraine \(recordedfuture.com\)](#))

January 24, 2022 – In a reported “first for ransomware,” a hacktivist group called the Belarusian Cyber Partisans claims credit for a cyberattack against the country’s railway system, reportedly in an attempt to impede Russian military movements into Belarus. The group demands the release of 50 political prisoners in need of medical attention and no Russian troops on Belarusian territory. It is said to be the

first use of ransomware for purposes of genuine, nongovernmental political activism. ([Cyberattack Targets Belarus' Rail Network To Slow Flood Of Russian Forces Into The Country \(thedrive.com\); Why the Belarus Railways Hack Marks a First for Ransomware | WIRED](#))

January 24, 2022 – The Defense Information Systems Agency (DISA) awards a \$6.8 million contract to Booz Allen Hamilton to produce a Thunderdome Prototype, “a zero trust security solution,” within six months. In July, the contract is extended for six months so that the prototype can include SIPRNet. ([News \(disa.mil\)](#))

January 28, 2022 – Responding to a reporter asking about U.S. preparedness for a potentially hostile Russian action, CJCS Mark Milley says: “With respect to your question about the homeland and cyber and all of that, we have capabilities – I’m not going to go into them here at the microphone – but we’ve got a significant amount of capabilities to defend and do whatever is necessary to protect the homeland.” ([Secretary of Defense Austin and Chairman of the Joint Chiefs of Staff Gen. Milley Press Briefing > U.S. Department of Defense > Transcript](#))

January 28, 2022 – An article in *Politico* highlights Western concerns about a major cyber conflict erupting over Ukraine and its potential future ramifications. “In a full-scale cyber assault, Russia could take down the power grid, turn the heat off in the middle of winter and shut down Ukraine’s military command centers and cellular communications systems. A communications blackout could also provide opportunities for a massive disinformation campaign to undermine the Ukrainian government.” Jonathan Reiber, chief strategy officer for cyber policy in the Office of the Secretary of Defense during the Obama administration, observes: “This may end up being the first declared hostility where cyberspace operations are a part of an integrated offensive military invasion.” ([Russian invasion of Ukraine could redefine cyber warfare - POLITICO](#))

January–February 2022 – Russian law enforcement agencies initiate an “unprecedented crackdown” on cybercrime, according to Mandiant later. The move closes a number of “top-tier carding shops” trafficking in stolen credit cards. Mandiant theorizes that Moscow wanted to indicate its willingness to cooperate with the West on cybercrime in case the West went along with Kremlin demands on Ukraine. By mid-March, carding shops make up the temporary loss although the year ends up not being a strong one for operators. ([Annual Payment Fraud Intelligence Report: 2022 \(recordedfuture.com\)](#))

February – Early May, 2022 – USCYBERCOM and Lithuania’s cyber forces run a joint three-month “hunt forward” operation, possibly involving other nations. It starts prior to Russia’s invasion of Ukraine. According to the U.S. agency, the aim is “to conduct defensive cyber operations” in search of “malicious cyber activity on key Lithuanian national defense systems and Ministry of Foreign Affairs’ networks alongside its allies.” The Command reports “This was the first shared defensive cyber operation between Lithuanian cyber forces and CNMF in their country.” Lithuanian Vice



Minister of National Defense Margiris Abukevicius says the “war against Ukraine has demonstrated that cyberattacks are an inseparable element of modern military campaigns” and preparations have to be made “during war and peace alike.” ([U.S. conducts first Hunt Forward Operation in Lithuania > U.S. Cyber Command > News; US seeking to understand Russia’s failure to project cyber power in Ukraine \(defensenews.com\)](#))

Hunt forward teams also coordinate with the U.S. European Command. “In addition to that work we did with Ukraine, with Ukrainians, we also deployed Air Force and Army cyber teams to Europe to support U.S. European Command directly. Those teams worked on cyber defense, worked very closely with those commands to ensure that all the theater networks were hardened in case there was an escalation or intrusions directed at the U.S.,” David Frederick, executive director of Cybercom, said at a virtual event hosted by GovConWire. ([US cyber teams prepped Eucom's networks for potential Russian attacks prior to Ukraine invasion \(defensescoop.com\)](#))

No date (2022) – (Possibly early February based on the following:) In a lengthy March 8 posting titled “Amazon’s cybersecurity assistance for Ukraine,” the company notes: “For several weeks, we have been partnering closely with Ukrainian IT organizations to fend off attacks and working with organizations in Ukraine, and around the world, to share real-time, relevant intelligence. As a result, our teams have seen new malware signatures and activity from a number of state actors we monitor.” The posting continues: “Our security teams are sharing this intelligence with governments and IT organizations that we partner closely with from Europe, North America, and around the world to equip critical infrastructure owners and operators with additional information to protect their facilities.” ([Amazon’s cybersecurity assistance for Ukraine \(aboutamazon.com\)](#))

February 3, 2022 – Pentagon spokesman John Kirby says Russia is planning a “fake attack by Ukrainian military or intelligence forces” incorporating “a very graphic propaganda video” in order to justify a Russian invasion of Ukraine. Kirby says the information is based on declassified intelligence. It is another instance of the selective release of sensitive information to try expose and disrupt Russian intentions. ([US alleges Russia planning false flag operation against Ukraine using 'graphic' video | CNN Politics](#))

February 7, 2022 – As reported later by Recorded Future, on around this date “Directorate ‘K’ of the Russian Ministry of Internal Affairs seizes the domains of at least 4 ... Russian-language dark web and special-access sources that facilitated cybercriminal activity.” They are: SkyFraud, Ferum Shop, Trump’s Dumps, and UAS Shop (each described in the report). ([Dark Covenant 2.0: Cybercrime, the Russian State, and the War in Ukraine \(recordedfuture.com\)](#))

February 8, 2022 – Contributing to the pre-war debate on whether Russia plans to use cyberattacks against Ukraine and what their impact would be, cyber experts Lennart Maschmeyer and Nadiya Kostyuk argue in *War on the Rocks* that there is no such

thing as “cyber ‘shock and awe’.” “Our research shows that cyber operations have remained irrelevant on the battlefield, while standalone operations to weaken Ukraine through election interference, critical infrastructure sabotage, and economic disruption largely failed to contribute to Russia’s strategic goals of making Ukraine abandon its pro-European Union and pro-NATO foreign policy. Consequently, current fears of cyber warfare defy not only Russia’s track record in Ukraine, but also strategic logic. Given that Russia’s cyber operations have failed to produce significant strategic value to date, why would we expect this to suddenly change now?” ([There Is No Cyber ‘Shock and Awe’: Plausible Threats in the Ukrainian Conflict - War on the Rocks](#))

February 11, 2022 – Gen. Paul Nakasone recalls later: “11th of February, I stood up our task force at NSA and Cyber Command, 24 by 7, because we knew that the invasion was coming soon.” ([‘Something Was Badly Wrong’: When Washington Realized Russia Was Actually Invading Ukraine - POLITICO](#))

February 11, 2022 – A Western journalist in Kyiv describes the personal impact of the cyber battles going on at the time: “On Friday [February 11], the U.S. and United Kingdom told its citizens to depart Ukraine, warning that a preface to a Russian attack would be a staged event to destabilize the country and spark armed conflict. By the time I left on Saturday, on the last KLM flight out of Kyiv, I had personally been feeling the impact of the ongoing hybrid conflict for more than a week. I had switched out one of my SIM cards to a local number when the problems began. They came as minor frustrations first — a slow connection, an unplanned reboot, a dropped phone call. Then I began receiving a slew of phishing emails on a scale I have never before experienced. I received a call from a Ukrainian number (no one but the photographer I worked with had the number) and a two-minute voicemail of faint clicking sounds. Maybe I was just being paranoid. But no fewer than four individuals from Ukraine, and a handful of people I spoke with abroad, began our phone calls by greeting the Russians who, they said, were no doubt listening. One woman in Donbas, reached by phone, quickly hung up, citing her fears over Russian interception. ¶ Whether on the front lines or not, Ukrainians live with the constant knowledge that their systems and technology and borders are under siege, that at the moment of a military action against their country, the internet will likely go dark, their connection to the world severed.” ([‘Kill Your Commanding Officer’: On the Front Lines of Putin’s Digital War With Ukraine - POLITICO](#))

February 13, 2022 – The CEO of Fractal Analytics Inc., based in New York, holds an emergency remote meeting with dozens of employees living in Ukraine. The purpose is to determine whether anyone wants to leave the country and whether there are any other steps the company should take to prepare for a military crisis. The experience is later described in a media account as emblematic of growing corporate concerns worldwide for the safety of workers and continuity of operations in case of a Russian invasion. ([Russia-Ukraine Invasion: Inside One Tech Company’s Attempt to Evacuate Employees - WSJ](#))

February 14, 2022 – Russia has boosted its military capability along the border with Ukraine, as well as in the Belarus area that borders Ukraine, according to Pentagon Press Secretary John Kirby. Cyber is one area where assets have been added. ([Putin Adds Military Capabilities in Belarus, Russian Border With Ukraine, Kirby Says > U.S. Department of Defense > Defense Department News](#))

February 14-23, 2022 – Among Russia’s cyber activities immediately preceding (and sometimes continuing after) the invasion are “DDoS attacks against public information resources and banking institutions, phishing attacks on government authorities and CIFs [critical infrastructure facilities], spreading of malware, infiltration and vandalism of public and private networks,” according to a May 2022 report by Dmytro Dubov, head of Ukraine’s International Centre for Defense and Security. (Dmytro Dubov, “Russia’s in Ukraine: The War in Cyberspace” (Series No. 2)

February 14, 2022 – Accenture Cyber Threat Intelligence (ACTI) issues a report on Ukraine that names several groups as currently among the most active in Ukraine and Eastern Europe: SANDFISH (a.k.a. Sandworm, TeleBots, Quedagh, BlackEnergy, Voodoo Bear, TEMP.Noble, GreyEnergy); WINTERFLOUNDER (a.k.a. Gamaredon Group, Calisto Group, Dancing Salome); WALLEYE (a.k.a. Zebrocy, Earworm). ([Global Incident Report: Russia Ukraine Crisis | Accenture](#))

February 14, 2022 – Microsoft later reports: “Odessa-based critical infrastructure compromised by likely Russian actors.” ([An overview of Russia’s cyberattack activity in Ukraine \(microsoft.com\)](#))

February 15, 2022 – Ukraine’s Center for Strategic Communications reports that the Ministry of Defence and the Armed Forces of Ukraine have been targeted by cyberattacks. ([Attention: there is no threat to the funds of privatbank depositors - Center for Strategic Communications \(spravdi.gov.ua\)](#))

February 15, 2022 – A lengthy report in *Politico* explores Russia’s long-running cyber activities in Ukraine: “The Russians have for nearly a decade used Ukraine as a proving ground for a new and highly advanced type of hybrid warfare — a digital-meets-traditional kind of fighting defined by a reliance on software, digital hardware and cognitive control that is highly effective, difficult to counter and can reach far beyond the front lines deep into Ukrainian society. It is a type of high-tech conflict that many military experts predict will define the future of war. It has also turned Ukraine, especially its eastern provinces, but also the capital, into a bewildering zone of instability, disinformation and anxiety.

“The Russians and their proxies have used digital technology on the battlefield not only to assist artillery in rapidly acquiring and engaging targets, but also to disrupt communications and wage psychological warfare, like sending threatening text messages to soldiers. Beyond the front lines, Russian efforts have knocked out government websites and spread damaging disinformation in towns and cities across the country. Digital warfare has threatened more of Ukrainian

society since 2021 than traditional munitions.” ([‘Kill Your Commanding Officer’: On the Front Lines of Putin’s Digital War With Ukraine - POLITICO](#))

February 15, 2022 – The same *Politico* piece (previous entry) quotes Oleksandr Danylyuk, former secretary of Ukraine’s National Security and Defense Council: “You can’t separate the military from the economy from the technology. That’s why they call it hybrid warfare. Russia, they own or operate Ukrainian cellular companies, banks, electricity ... They don’t need to hack anything. It’s a secret war conducted by agents of influence.” ([‘Kill Your Commanding Officer’: On the Front Lines of Putin’s Digital War With Ukraine - POLITICO](#))

February 15-16, 2022 – Ukraine’s banking sector is hit by DDoS attacks, which the U.K. government soon attributes to the GRU. ([UK assesses Russian involvement in cyber attacks on Ukraine - GOV.UK \(www.gov.uk\)](#); Rob Joyce slide at RSAC 2022)

February 16, 2022 – A detailed CISA alert about Russian state-sponsored cyber activity begins: “From at least January 2020, through February 2022, the Federal Bureau of Investigation (FBI), National Security Agency (NSA), and Cybersecurity and Infrastructure Security Agency (CISA) have observed regular targeting of U.S. cleared defense contractors (CDCs) by Russian state-sponsored cyber actors. The actors have targeted both large and small CDCs and subcontractors with varying levels of cybersecurity protocols and resources.” ([Russian State-Sponsored Cyber Actors Target Cleared Defense Contractor Networks to Obtain Sensitive U.S. Defense Information and Technology | CISA](#))

February 17, 2022 – Moscow warns it will be “forced to respond” with military-technical measures if Washington fails to guarantee Ukraine will never be allowed to join NATO. ([An overview of Russia’s cyberattack activity in Ukraine \(microsoft.com\)](#))

February 17, 2022 – Gen. Paul Nakasone later recalls a phone conversation with Chairman of the Joint Chiefs Mark Milley: “The 17th of February, I fly home for a speech in my hometown of St. Paul, Minnesota, and it’s been really cold — if you’ve ever been in Minnesota, February is a cold month — and the chair calls me about 5:30 at night, Central Time. It’s a pretty sensitive call, so I asked my colleagues, “Hey, can you just step out of the car for a second so I can talk to the chair?” My guys later tell me, “So it is the coldest day of the year, and we’re wondering how long the chairman’s going to talk to you.” The chair’s like, “OK, so just one more time — what do you think?” I said, “It’s coming soon, chairman. I know it.” He says, “Yep. I believe it as well.” This is just this confidence that we have collectively on the 17th of February.” ([‘Something Was Badly Wrong’: When Washington Realized Russia Was Actually Invading Ukraine - POLITICO](#))

February 17, 2022 – Microsoft later reports: “Suspected Russian actors present on critical infrastructure networks in Sumy.” ([An overview of Russia’s cyberattack activity in Ukraine \(microsoft.com\)](#))



February 17, 2022 – Ukraine’s Parliament amends its Data Protection Law to permit cloud storage of government data. Within 10 weeks and with outside private sector support, much of the government’s critical data is copied to the cloud from on-site servers. (Microsoft, “Defending Ukraine,” [Defending Ukraine: Early Lessons from the Cyber War \(microsoft.com\)](#), p. 5)

February 17, 2022 – On this date if not earlier, a Ukrainian energy company experiences an initial attack by Russian-origin malware, investigators later determine. They say it is just one part of a larger assault designed to take down part of Ukraine’s energy grid. The next apparent hit involves HermeticWiper on February 23 (see entry below), followed by a bigger attack on April 8 (see entry). ([Industroyer2: How Ukraine avoided another blackout attack \(techtarget.com\)](#))

February 17-18, 2022 – According to cited press reports, “During the night of 17-18 February, cellphone service in several government-held cities in eastern Ukraine experienced disruptions for hours. The phone company attributed it to ‘vandalism’ of the fiber optic lines. Ukrainian journalist Margo Gontar quoted the Ukrainian Interior Ministry as having said ‘This is part of Russia’s plan to destabilize situation in Ukraine. We must understand sabotage at communications facilities will continue.’” ([Global Incident Report | Accenture](#))

February 18, 2022 – New Zealand issues a General Security Advisory: “The National Cyber Security Centre (NCSC) encourages Aotearoa New Zealand’s nationally significant organisations to consider and strengthen their cyber security readiness in response to heightened tensions between Russia and Ukraine.” ([NCSC - General Security Advisory: Understanding and preparing for cyber threats relating to tensions between Russia and Ukraine](#))

February 19, 2022 – CISA issues a alert that “In light of developing Russia-Ukraine geopolitical tensions, the risk of foreign influence operations affecting domestic audiences has increased.” ([Preparing for and Mitigating Foreign Influence Operations Targeting Critical Infrastructure \(cisa.gov\)](#))

February 19, 2022 – *Politico* reports: “The U.S. and its allies poured tens of millions of dollars during the past seven years into helping Ukraine shore up its electric grid against a Russian cyberattack, while Ukrainian authorities launched a massive program to harden their cyber defenses. Nobody thinks it will be enough.” That assistance includes \$38 million USAID announced in 2020 it would invest in the country’s cybersecurity resilience over a four-year period. ([Despite years of preparation, Ukraine’s electric grid still an easy target for Russian hackers - POLITICO](#))

February 20, 2022 – Accenture Cyber Threat Intelligence (ACTI) names the following threat actors or groups active in Ukraine: vlakyla, GodLevel, an3key, and Free Civilian. ([Global Incident Report: Deep Web Database and Network Access Sales Affecting Russia Ukraine Dispute | Accenture](#))

February 2022 – (Approx.) Beginning shortly prior to the war, Ukraine is hit by “relentless and destructive Russian cyberattacks,” according to a later Microsoft blog entry by Vice President Tom Burt. “Starting just before the invasion, we have seen at least six separate Russia-aligned nation-state actors launch more than 237 operations against Ukraine – including destructive attacks that are ongoing and threaten civilian welfare. The destructive attacks have also been accompanied by broad espionage and intelligence activities. The attacks have not only degraded the systems of institutions in Ukraine but have also sought to disrupt people’s access to reliable information and critical life services on which civilians depend, and have attempted to shake confidence in the country’s leadership. We have also observed limited espionage attack activity involving NATO member states, and some disinformation activity.” ([The hybrid war in Ukraine - Microsoft On the Issues](#))

February 21, 2022 – President Putin recognizes the independence of Ukraine’s eastern separatist regions. ([An overview of Russia’s cyberattack activity in Ukraine \(microsoft.com\)](#))

February 21, 2022 – British Defence Secretary Ben Wallace declares in the House of Commons that the U.K. is prepared to use cyber to respond to any attacks on British computer networks by Russia. “I’m a soldier – I was always taught the best part of defence is offence,” he adds. ([Ukraine: UK ready to launch retaliatory cyber-attacks on Russia, defence secretary tells MPs | The Independent](#))

February 23, 2022 – Microsoft’s Threat Intelligence Center detects a new instance of the malware HermeticWiper (which it labels “FoxBlade”) and within hours notifies the Ukrainian government of an apparent threat to its ministries and financial institutions, then updated the company’s detection systems to block the malware. At the request of Deputy National Security Adviser Anne Neuberger, Microsoft then shares the information with other governments in the region. According to the *New York Times*, this marks a new level of activity by private sector companies in the global cybersecurity arena. ([Tech Companies Help Defend Ukraine Against Cyberattacks - The New York Times \(nytimes.com\)](#); Rob Joyce slide at RSAC 2022)

Victor Zhora, deputy chairman of Ukraine’s State Service of Special Communications and Information Protection (SSSCIP) later credits Microsoft and ESET for swiftly providing authorities with large amounts of telemetry data accumulated from their major presence on Ukrainian networks. CERT-UA also played a big part by detecting the malware and notifying the targets. ([Industroyer2: How Ukraine avoided another blackout attack \(techtarg.com\)](#))

The *New York Times* explores the public/private partnership in more detail the following week:

“After years of discussions in Washington and in tech circles about the need for public-private partnerships to combat destructive cyberattacks, the war in Ukraine is stress-testing the system. The White House, armed with intelligence from the National Security Agency and United States Cyber Command, is overseeing classified briefings on Russia’s cyberoffensive plans. Even if American intelligence

agencies picked up on the kind of crippling cyberattacks that someone — presumably Russian intelligence agencies or hackers — threw at Ukraine's government, they do not have the infrastructure to move that fast to block them.

"We are a company and not a government or a country,' Brad Smith, Microsoft's president, noted in a blog post issued by the company on Monday, describing the threats it was seeing. But the role it is playing, he made clear, is not a neutral one. He wrote about 'constant and close coordination' with the Ukrainian government, as well as federal officials, the North Atlantic Treaty Organization and the European Union.

"I've never seen it work quite this way, or nearly this fast,' Mr. Burt said. 'We are doing in hours now what, even a few years ago, would have taken weeks or months.'

"The intelligence is flowing in many directions.

"Company executives, some newly armed with security clearances, are joining secure calls to hear an array of briefings organized by the National Security Agency and United States Cyber Command, along with British authorities, among others. But much of the actionable intelligence is being found by companies like Microsoft and Google, who can see what is flowing across their vast networks.

"Mr. Biden's aides often note that it was a private firm — Mandiant — that found the 'SolarWinds' attack 15 months ago, in which one of Russia's most cybersavvy intelligence agencies, the S.V.R., infiltrated network management software used by thousands of U.S. government agencies and private businesses." ([Tech Companies Help Defend Ukraine Against Cyberattacks - The New York Times \(nytimes.com\)](https://www.nytimes.com/2022/02/23/us/politics/cyberattacks-ukraine.html))

February 23, 2022 – Cybersecurity firms SentinelLabs and Broadcom Software report that HermeticWiper is being used against organizations in Ukraine. (CrowdStrike designates the attackers as DriveSlayer.) ESET also reports intensive hacking aimed at the country. SentinelLabs indicates the malware's target is Windows devices while Broadcom notes that it "has some similarities to the earlier WhisperGate wiper attacks against Ukraine, where the wiper was disguised as ransomware." (CISA, [Update: Destructive Malware Targeting Organizations in Ukraine | CISA; Ukraine computers hit by data-wiping software as Russia launched invasion | Reuters](https://www.cisa.gov/news-events/alerts/2022/02/23/ukraine-computers-hit-by-data-wiping-software-as-russia-launched-invasion); Rob Joyce slide at RSAC 2022; House Homeland Security Subcommittee on Cybersecurity, Infrastructure Protection and Innovation, hearing on Russian cyber threats, 4-5-22; [A year after Russia's invasion, the scope of cyberwar in Ukraine comes into focus | CyberScoop](https://www.cyberscoop.com/ukraine-cyberwar-focus/))

February 23, 2022 – CISA advises that various agencies "have identified that the actor known as Sandworm or Voodoo Bear is using a new malware, referred to here as Cyclops Blink. The [U.K.'s] NCSC, CISA, and the FBI have previously attributed the Sandworm actor to the Russian General Staff Main Intelligence Directorate's Russian (GRU's) Main Centre for Special Technologies (GTsST)." The alert continues: "Cyclops Blink appears to be a replacement framework for the VPNFilter malware exposed in 2018, and which exploited network devices, primarily small office/home

office (SOHO) routers and network attached storage (NAS) devices.” ([New Sandworm Malware Cyclops Blink Replaces VPNFilter | CISA](#))

February 23 – April 8, 2022 – During this period, Microsoft reports seeing “evidence of nearly 40 discrete destructive attacks that permanently destroyed files in hundreds of systems across dozens of organizations in Ukraine.” Over 40% of these attacks are aimed at critical infrastructure sectors, while 32% hit government organizations. ([An overview of Russia’s cyberattack activity in Ukraine \(microsoft.com\)](#))

Pre-February 24, 2022 – Cisco later writes: “As the invasion approached, there were other minor events, but none that had any appreciable impact. These were distributed denial-of-service (DDoS) or unsuccessful wiper attacks and an unconfirmed manipulation of Border Gateway Protocol (BGP) routing. Our assessment is that the best of Russia’s cyber capability was focused elsewhere, likely in espionage activities trying to understand the global response to Russia’s invasion. Regardless of the reason, there were no major cyber incidents against Ukraine in the days leading up to the invasion.” ([Cisco stands on guard with our customers in Ukraine - Cisco Blogs](#))

February 23-24, 2022 – A Russian cyberattack on Viasat, Inc., a satellite broadband service and secure networking provider based in California, disrupts service for tens of thousands of users. British and U.S. intelligence later (May 10) announce Russia is to blame and that they believe the main target was Ukraine’s military. British Foreign Secretary Liz Truss describes “clear and shocking evidence of a deliberate and malicious attack by Russia against Ukraine which had significant consequences on ordinary people and businesses in Ukraine and across Europe.” The attack utilized a form of malware called “AcidRain.” ([US and allies blame Russia for Viasat hack ahead of Ukraine invasion \(c4isrnet.com\)](#); [How Russia telegraphed invasion of Ukraine in space and online \(defensenews.com\)](#); [Russia behind cyber attack with Europe-wide impact an hour... - NCSC.GOV.UK](#); [Cyberattacks quietly launched by Russia before its invasion of Ukraine may have been more damaging than intended | Business Insider India](#); Rob Joyce slide at RSAC 2022)

Director of National Intelligence Avril Haines tells the Senate Armed Services Committee later she believes the aim of the attack was to disrupt Ukrainian military command and control capabilities but that it had an “outsized impact” that “ended up affecting a much broader set of VSATs, essentially, you know, very small terminals outside of Ukraine, including in Europe.” ([OPEN/CLOSED\\* To receive testimony on worldwide threats \(senate.gov\)](#))

Looking back a year later, Anne Neuberger, deputy national security adviser for cyber and emerging technology, says “That was the first time the European Union came together to attribute a cyberattack and call out Russia. This was a big deal in terms of cyber norms.” ([Biden’s cyber promises, two years later - The Washington Post](#))

Seeming to present a less severe reading of the Viasat event, the German government describes its effects as “cyber collateral damage” with no additional



impact on the country's critical infrastructure. A senior Ukrainian cyber official initially claims the effects were "huge" but later backs away from the comment. ([Why Cyber Dogs Have Yet to Bark Loudly in Russia's Invasion of Ukraine - Texas National Security Review \(tnsr.org\)](#); [Viasat Hack "Did Not" Have Huge Impact on Ukrainian Military Communications, Official Says \(substack.com\)](#))

A year later, Bloomberg describes the Viasat attack as a wakeup call for the satellite industry. (<https://www.bloomberg.com/features/2023-russia-viasat-hack-ukraine/>)

February 24, 2022 – (Date approx.) German turbine manufacturer Enercon GmbH loses remote control of 5,800 wind turbines – “collateral damage” from an attack on a satellite company (presumably Viasat) in February, Enercon reports later. ([European Wind-Energy Sector Hit in Wave of Hacks \(wsj.com\)](#))

February 24, 2022 – Russian military forces invade Ukraine. Early in the morning, Russian TV broadcasts a lengthy speech by President Putin justifying the “special military operation” and warning: “no one should have any doubts that a direct attack on our country will lead to defeat and horrible consequences for any potential aggressor.” ([‘No other option’: Excerpts of Putin’s speech declaring war | Russia-Ukraine war News | Al Jazeera](#))

February 24, 2022 – Simultaneous with the land invasion, Russian entities conduct “wiper attacks” [HermeticWiper] (see also entries for February 23) on the country's computer networks. Initially, most observers are surprised by what appears to be the absence of an accompanying series of crippling cyber strikes against Ukrainian infrastructure. ([Tech Companies Help Defend Ukraine Against Cyberattacks - The New York Times \(nytimes.com\)](#); [How the cloud saved Ukraine’s data from Russian attacks \(c4isrnet.com\)](#))

According to Symantec, the targets are the financial, defense, aviation, and IT services sectors

Microsoft later reports seeing “several examples of computer network operations and military operations seeming to work in tandem against a shared target set, though it is unclear if there is coordination, centralized tasking or merely a common set of understood priorities driving the correlation. At times, computer network attacks immediately preceded a military attack, but those instances have been rare from our perspective. The cyber operations so far have been consistent with actions to degrade, disrupt, or discredit Ukrainian government, military, and economic functions, secure footholds in critical infrastructure, and to reduce the Ukrainian public’s access to information.” ([An overview of Russia’s cyberattack activity in Ukraine \(microsoft.com\)](#))

February 24, 2022 on – Among Russia’s cyber activities immediately preceding (and sometimes continuing after) the invasion are a series of emails and simple notification service messages, cyberattacks against critical infrastructure facilities, the defacing of websites, DDoS attacks, and attempts to access internal information systems, according to a May 2022 report by Dmytro Dubov, head of Ukraine’s

International Centre for Defense and Security. (Dmytro Dubov, “Russia’s in Ukraine: The War in Cyberspace” (Series No. 2)

February 24, 2022 – According to a Twitter message cited by Accenture, “In the early hours of 24 February, residents in the separatist-occupied city of Donetsk reported an electricity blackout and spotty Internet coverage as armored columns moved into the city, according to social media accounts.” ([Global Incident Report | Accenture](#))

February 24, 2022 – As of this morning, Hacker forums in Ukraine are already sending out calls for volunteers. One post by a cybersecurity company founder who says he was asked by a senior Defense Ministry official to send it read: “Ukrainian cybercommunity! It's time to get involved in the cyber defense of our country.” In an interview, Yegor Aushev describes plans for defensive and offensive units. Other sources confirm the Defense Ministry’s involvement. Aushev says by the end of the day he has already received hundreds of applicants. ([Ukraine calls on hacker underground to defend against Russia - The Jerusalem Post \(jpost.com\)](#))

February 24-26, 2022 – In this timeframe, Yegor Aushev reportedly reaches out to Mykhailo Federov, Ukraine’s 31-year-young Minister of Digital Transformation, proposing the idea of a cyber volunteer army. ([Cyber-Reports-2022-06-IT-Army-of-Ukraine.pdf \(ethz.ch\)](#))

February 24, 2022 – Along with various Russian government websites, some major banks such as Sberbank and Alfabank are targeted by DDoS attacks. Russia responds by apparently trying to geofence the sites to block international users. ([Russia seems to geofence government sites after DDoS attacks, partially blocks Facebook and Twitter - DCD \(datacenterdynamics.com\)](#))

February 24, 2022 – Kharkiv and Mariupol experience Internet disruptions while the Russia-based NGO Internet Protection Society reports Kyiv, Kharkiv, Donetsk, Kherson, Vinnitsya, Luhansk, Sumy, and Khmelnytskyi are having connectivity problems. (<https://netblocks.org/reports/internet-disruptions-registered-as-russia-moves-in-on-ukraine-W80p4k8K>; [Global Incident Report | Accenture](#))

February 24, 2022 – Within hours of the invasion, Liam Maxwell, director of government transformation at Amazon Web Services (AWS), meets in London with a Ukrainian official and “literally [writes] down on a piece of paper” what Ukraine needs to do to protect its digital assets, Maxwell tells the Financial Times later. ([What Ukraine’s cyber defence tactics can teach other nations | Financial Times \(ft.com\)](#); [Whatever Happened to Russia’s Vaunted Cyberoffensive? \(foreignpolicy.com\)](#))

February 24, 2022 – In the course of White House remarks after Russia’s invasion, President Biden says, “Let me also repeat the warning I made last week: If Russia pursues cyberattacks against our companies, our critical infrastructure, we are prepared to respond. For months, we have been working closely with our private — with the private sector to harden their cyber defenses, sharpen our ability to

respond to Russian cyberattacks as well.” (White House transcript of remarks, 2-24-22, [Remarks by President Biden on Russia's Unprovoked and Unjustified Attack on Ukraine | The White House](#))

February 24, 2022 – President Biden has been briefed on numerous options for “massive cyberattacks” against Russia, according to NBC News. “Among the options: disrupting internet connectivity across Russia, shutting off electric power, and tampering with railroad switches to hamper Russia’s ability to resupply its forces, three of the sources said.” The White House denies the report the same day. ([Biden has been presented with options for massive cyberattacks against Russia \(nbcnews.com\)](#); [White House Denies Mulling Massive Cyberattacks Against Russia | Threatpost](#))

February 24, 2022 – The United States and a number of allies impose “sweeping financial sanctions and stringent export controls” on Russia that “will have a profound impact” on its economy, the White House announces. “The unprecedented export control measures will cut off more than half of Russia’s high-tech imports, restricting Russia’s access to vital technological inputs, atrophying its industrial base, and undercutting Russia’s strategic ambitions to exert influence on the world stage.” ([FACT SHEET: Joined by Allies and Partners, the United States Imposes Devastating Costs on Russia | The White House](#))

February 24, 2022 on – Following Russia’s invasion, USAID’s Cybersecurity for Critical Infrastructure in Ukraine program, launched in May 2020, begins funding “technical experts to provide hands-on support to essential service providers within the Ukrainian government including government ministries and critical infrastructure operators to identify malware and restore systems after an incident has occurred.” According to an agency fact sheet, “This support builds on long standing USAID support building cyber resilience among regional utilities, particularly in the energy sector. Amid Russia’s invasion, USAID has also provided more than 6,750 emergency communications devices, including satellite phones and data terminals, to essential service providers, government officials, and critical infrastructure operators in key sectors such as energy and telecommunications.” ([Cybersecurity | Ukraine | Fact Sheet | U.S. Agency for International Development \(usaid.gov\)](#))

February 24, 2022 – Twitter messages indicate the main Russian government website was inaccessible in the evening along with other Kremlin and Parliament sites. A spokesperson denies any attacks occurred. Brief DDoS activity also takes place on the RT media site. ([Global Incident Report | Accenture](#))

February 24, 2022 – Military analyst Rob Lee (@RALee) tweets: “Of the things that have surprised me thus far, I thought we’d see heavier use of electronic warfare and cyber tools to disrupt Ukrainian command, control, and communications. I also feared we’d see a heavier use of fires, including MLRS blanketing areas with cluster munitions.” Cyber expert Dmitri Alperovitch (@DALperovitch) replies: “Same. I expected them to shut down cell networks and Internet and try to prevent some of

the horrible videos and photos from getting out. This just hasn't been the shock and all campaign that the Russians had capacity to execute." ([Twitter](#); [SITREP Ukraine | Accenture](#))

February 24, 2022 on – (Approx.) Among other U.S. departments and agencies, the relatively tiny Defense Innovation Unit (DIU) reacts swiftly to the invasion. "As soon as we saw the events unfold and we saw the invasion was happening," Director Mike Brown says later, "with the U.S. getting involved to help NATO allies — we immediately highlighted the commercial technologies that we thought could be useful so that they would be able to be put on the security assistance lists that are provided to Ukraine and make sure that European Command, the force that's working most closely with NATO, would have access to those."

Commercial technologies are featuring prominently in DIU's effort, Brown tells FedScoop, including secure communications tools, drones, and satellite imagery. Synthetic aperture radar (SAR), for example, which utilizes space-based sensors, has allowed Ukraine to accomplish "some pretty damaging effects." By using radar images instead of optical, "you can see through cloud, and you can see at night – and this has been a game-changer in Ukraine." U.S. intelligence was able from the start to use these technologies to prove that Russia was building up its forces and planned to invade. Since then, the U.S. has been able to combine them with AI "to actually do battlefield assessments."

Because the technology is commercially manufactured, Brown tells FedScoop, it is unclassified, which has made it possible to share it rapidly with Ukrainians and other allies. "They can do battlefield damage assessments, as soon as missiles are flying in the air. So, the Ukrainians can get a color-coded view using commercial technology of what is the damage that's just occurred because these missiles have flown. That's an example of kind of a game-changing technology, in terms of closer to real-time situational awareness."

Brown underscores the impact of the current conflict on future war planning: "We're seeing the change in front of our eyes in Ukraine — commercial technology is going to be more important and used in some new and different ways ... I think it's underscoring how important the mission of DIU is. As we think about warfare evolving over the next couple of decades, there's going to be more and more of these commercial technologies that are going to be applied in warfare." ([Exiting DIU director urges Pentagon to refresh how it adopts commercial tech for future wars \(fedscoop.com\)](#))

February 24, 2022 on – Cisco reports later: "Once the invasion began, things moved very quickly. The amount of information to be processed about what was happening in Ukraine exploded ... Early on, we deployed Secure Endpoint in some new environments under a demo license that was set to expire. When we went to the business to extend it, the decision was made to extend all security licenses for all Cisco customers in Ukraine. During this chaotic period, no customer would lose protection because they were dealing with more important matters than license renewals."



“Additionally, we extended a new offer to critical organizations in Ukraine: Talos [Cisco’s threat intelligence division] would monitor their Secure Endpoint configurations, modify them based on our intelligence and aggressively hunt in their environments for threats at no cost. For each organization that accepted this offer, we assigned a set of engineers to manage the protections and configurations and two hunters from Talos to work with that specific data set.” ([Cisco stands on guard with our customers in Ukraine - Cisco Blogs](#))

February 24, 2022 on – Ukraine’s surprisingly robust response to Russian cyberattacks is explained a year later by the NSA’s Rob Joyce at a CSIS event (as reported in this excerpt from Breaking Defense):

“They were very resilient. How did they get that? They got there because they practiced for years,” he said. “They’ve gotten to the point where, you know, the Ukrainian sysadmins knew they had to have backups, and when they got a [data destroying] wiper virus they shrugged their shoulders, they cleaned the machine, they reloaded from backup and they moved on.”

What’s more, he said, “around the invasion ... they got an uplift from the US government providing resources, but [also] a lot of pro bono industry support, to make them much harder targets.” [A critical move was to host data on cloud servers in the West.] “You now went from two people who were maintaining and operating those servers to teams of hundreds or thousands,” Joyce said.

[He added that making contact with Western service providers was far easier than with scattered operatives in Ukraine]. “I wasn’t going to find those two server admins in in Ukraine and be able to help them directly like that.” ([US tech firms should wargame response if China invades Taiwan, warns NSA cybersecurity chief - Breaking Defense](#))

February 24, 2022 on – Early in the campaign, Russia and Ukraine begin to target satellite capabilities, according to U.S. Chief of Space Operations Gen. Chance Saltzman, speaking on the war’s first anniversary. “Right out of the gate, we saw both sides attacking satellite operations to degrade command and control. We see a lot of GPS interference to degrade those kinds of capabilities. So clearly if right out of the gate you’re trying to degrade those capabilities, you recognize that they are central to operations, that they are important to how a force fights in the modern environment ... It’s important to recognize just exactly what can go wrong if you don’t plan for that.” ([Space Force chief concerned about ‘backdoor’ for attacking satellite communications | DefenseScoop](#))

February 24, 2022 on – According to a later media report, “In the first phase of the war, Ukraine’s internet connectivity dropped about 20 per cent, said Simon Angus, director of the IP Observatory.” After that, “there was a kind of a status quo up until October,” Angus said. ([The battle to keep Ukraine connected to the internet amid Russian missile attacks - ABC News](#))

No date (2022) – Shortly after Russia’s invasion, in what will become a pattern, a Ukrainian cybersecurity startup named Hacken adapts one of its anti-DDoS tools, disBalancer,

to enable it to launch DDoS attacks. “We have made good strong hits, and a lot of websites don't work,” says Dmytro Budorin, the CEO of Hacken. ([Russia Is Being Hacked at an Unprecedented Scale | WIRED](#))

February 25, 2022 – Early in the morning Anonymous TV (@YourAnonTV) tweets: “We are convinced that sanctions against Putin's criminal regime will have no effect. We call on countries that support #Ukraine to sever ties with #Russia and expel Russian ambassadors. #Anonymous will intensify cyber attacks on the Kremlin this afternoon.(Moscow Time) #OpRussia.” ([Twitter](#))

February 25, 2022 – (Approx.) Shortly after Anonymous announces (on February 25) it will target Russian state entities, various Russian government websites go offline and confidential materials from the Ministry of Nuclear Safety are leaked to the Mega file-sharing site, according to one published account. ([What the War in Ukraine Means - Infosecurity Magazine \(infosecurity-magazine.com\)](#))

February 25, 2022 – The ransomware group Conti, reported to have ties to Russian intelligence, announces its “full support” of the Russian government and promises to use “all possible resources to strike back at the critical infrastructures” of any entity that organizes a cyberattack “or any war activities against Russia.” CISA and the FBI in September reported the group had been involved in “more than 400 attacks against mostly U.S. targets between spring 2020 and spring 2021,” according to CyberScoop. ([Conti ransomware group announces support of Russia, threatens retaliatory attacks \(cyberscoop.com\)](#))

February 26, 2022 – Accenture later reports: “Throughout the day ... numerous Russian government and state media sites were unavailable. At midnight, Russian state media outlet RIA Novosti reported (translated): ‘The Digital Ministry informs you that it is encountering an unprecedented scale of cyber-attacks, including a series of professional targeted attacks against the State Services portal. Security center specialists are successfully repelling all the attacks.’” ([SITREP Ukraine | Accenture](#))

February 26, 2022 – Ukraine's Minister of Digital Transformation, Mykhailov Fedorov, tweets: “We are creating an IT army. We need digital talents. All operational tasks will be given here: <https://t.co/Ie4ESfxoSn>. There will be tasks for everyone. We continue to fight on the cyber front. The first task is on the channel for cyber specialists.” ([Twitter](#))

February 26, 2022 – The IT Army posts its first Telegram message: “IT ARMY of Ukraine. Task # 1 We encourage you to use any vectors of cyber and DDoS attacks on these resources.” There follows a list of 22 commercial and nine Russian government websites. About two hours later, an almost identically worded post appears on the official Telegram channel of the Ministry of Digital Transformation. (<https://archive.ph/SMt31>; [IT ARMY of Ukraine – Telegram \(archive.ph\)](#))

February 26, 2022 – CISA and FBI issue a joint Cybersecurity Advisory (CSA) on malware targeting Ukrainian organizations (it is updated on April 28, see below). ([AA22-057A Destructive Malware Targeting Organizations in Ukraine.pdf \(cisa.gov\)](#))

February 26, 2022 – Relevant to the ongoing speculation about Putin and Ukraine, cyber expert Dmitri Alperovitch tweets: “Putin/Russia getting completely isolated economically & diplomatically. The West is completely united. Even China is getting scared of secondary sanctions. The danger: Putin has very little to lose now. He is cornered. May go all out on economic and cyber retaliation.” ([Twitter](#))

February 27, 2022 – Ukrainian diplomatic posts around the world are taken down by a suspected Russian cyberattack. Embassy Washington spokesperson Volodymyr Reznichenko confirms the attack but withholds comment on the possible perpetrator. ([2022 Russia-Ukraine war — Cyber group tracker. Update 2. - Cyberknow - Medium](#))

February 27, 2022 – German Chancellor Olaf Scholz delivers a speech to the Bundestag declaring “February 24, 2022, marks a turning point in the history of our continent.” He pledges that Germany will set up a €100 billion fund to be drawn upon to modernize and upgrade the country’s military and will raise its defense spending to above 2% of GDP. (Nine months later, Scholz’s domestic critics begin to question the lack of concrete action, though media reports say that few doubt his sincerity.) ([Reden zur Zeitenwende \(bundesregierung.de\)](#); [Poorly equipped German army awaits financial reinforcement from Berlin | Financial Times \(ft.com\)](#))

February 27, 2022 – Twitter account @ContiLeaks begins leaking links to the logs of more than 60,000 of the group’s internal messages, giving threat intelligence researchers worldwide an unusual window into Conti’s activities. ([Who is Trickbot? \\* Cyjax](#))

February 27, 2022 – Citing Twitter, Accenture reports “the social media accounts of @itarmyofukraine and other groups posted numerous claims of cyber-attacks on Russian targets.” ([SITREP Ukraine | Accenture](#))

February 27, 2022 – Two days after Conti throws its support behind the Putin government’s invasion of Ukraine, an unidentified Ukrainian security researcher begins leaking tens of thousands of the group’s internal messages going back to January 21, 2021. Over the next two days, more messages and valuable source code are released, although the latter is password protected. (A different “researcher” soon breaks the password and makes the code available.) According to BleepingComputer, the messages describe various gang activities, “including previously unreported victims, private data leak URLs, bitcoin addresses, and discussions about their operations.” ([Conti ransomware's internal chats leaked after siding with Russia \(bleepingcomputer.com\)](#))

February 27, 2022 – Facebook parent company Meta says that it has uncovered attempts to hack into Ukrainian military and civilian officials’ accounts for purposes of

spreading disinformation. Meta closed the accounts and notified their owners. Twitter and YouTube report similar intrusions. Meta identifies the perpetrators as affiliates of Ghostwriter, a Belarusian group, which has reportedly been “heavily active” in Ukraine recently. ([Tech Companies Help Defend Ukraine Against Cyberattacks - The New York Times \(nytimes.com\)](#))

February 28, 2022 – Four days after the invasion, authorities in the Russian Republic of Bashkortostan produce a “Report on the Existence of Protest Moods” based on scrutiny of social media postings. The document, obtained in 2022 and published along with nearly 160,000 other such records by the *New York Times*, is reported to be part of the activity of Russia’s vast social surveillance operation overseen by the government’s Internet regulator, Roskomnadzor. ([Inside Russia’s Vast Surveillance State: ‘They Are Watching’ - The New York Times \(nytimes.com\)](#))

February 28, 2022 – Microsoft begins posting a blog to publicly document its increasing activity in connection with Ukraine events. ([Digital technology and the war in Ukraine - Microsoft On the Issues](#); [Tech Companies Help Defend Ukraine Against Cyberattacks - The New York Times \(nytimes.com\)](#))

February 28, 2022 – Ukrainian officials on social media ask readers for information on Russian cyber defense vulnerabilities; their Cyber Front chatbox is @stop\_russian\_war\_bot. ([SITREP Ukraine | Accenture](#))

February 28, 2022 – Anti-Russian hacktivists report they are targeting several entities, including: Sberbank, The Moscow Stock Exchange, the petroleum and machinery company Severnaya Kompaniya, the Russian Railways, the Russian contractor “promen48[.]ru,” the Joint Institute for Nuclear Research at Dubna State University, electric vehicle charging stations inside Russia, and Russian TV transmissions. ([SITREP Ukraine | Accenture](#))

February 28, 2022 – The website Ukrinform reports that Ukraine’s Ministry of Digital Transformation is saying the Russian FSB website is down and that Ukrainian and other “cybertroops are continuing their work.” ([Сайт ФСБ России «лег» – Минцифры \(ukrinform.ru\)](#))

February 28, 2022 – Ukrainian software engineers launch an online game called “Play for Ukraine” that “crowdsources and gamifies participation” in DDOS attacks against selected Russian government and media websites, according to a media report. The game is based on “2048,” a popular puzzle game. It is set up so that every player’s move contributes to an attack. “Our main goal is websites that serve the Russian army,” according to the Lviv-based team. “We ... rely on a steady torrent of automated traffic to knock target websites offline.” By mid-March, they report a milestone: 2,048 players have taken part, hitting more than 200 Russian websites. ([This game crowdsources cyberattacks against Russian websites \(fastcompany.com\)](#))



No date (2022) – According to a media report, numerous groups have been using apps and infrastructure to help Ukraine in its information war against Russia. One of the tools is a popular social face swapping app called Reface which the report says “has a large Russian userbase, and the developers have sent more than 13 million push notifications to the devices [of] its Russian users showing the real civilian damage caused in Ukraine by Putin’s military. The aim is to refute Moscow’s portrayal of the war. “MacPaw (Mac productivity) and BetterMe (health coaching) have also sent informational push notifications about the war to the devices of their Russian app users.” ([This game crowdsources cyberattacks against Russian websites \(fastcompany.com\)](#))

February 2022 – A new Telegram channel called Relocation.Guide launches to help Russians trying to leave the country. By October it has roughly 200,000 members and is being touted as one of the creative ways technology is being used to deal with the war in Ukraine. ([гайд в свободный мир \(relocation.guide\)](#); [This Telegram community helps Russians escape Putin’s draft - The Washington Post](#))

February 28, 2022 – Ukrainian Deputy Minister of Digital Transformation Mykhailo Fedorov writes to the Internet Corporation for Assigned Names and Numbers (ICANN) urging that it revoke certain Russ-associated domain names and SSL certificates, and shut down DNS root servers in the Russian Federation because of its invasion of Ukraine. ([Goran-Marby.pdf \(eump.org\)](#))

February 28, 2022 – According to later reports cited by Accenture, on this date a RIPE (Réseaux IP Européens) Network Coordination Center study determines that Ukraine’s physical internet infrastructure “has been mostly intact and functioning since the start of the conflict.” ([SITREP Ukraine | Accenture](#))

February 28, 2022 – Microsoft later reports: “Threat actor compromises a Kyiv-based media company.” ([An overview of Russia’s cyberattack activity in Ukraine \(microsoft.com\)](#))

February 28, 2022 – Google’s Threat Analysis Group (TAG) posts a quarterly bulletin (later updated on May 12) that includes reports of closing down several hundred YouTube channels with pro-Russian content and/or disinformation relating to Ukraine in February-March. ([TAG Bulletin: Q1 2022 \(blog.google\)](#))

February 28, 2022 – YouTube, Facebook, Instagram, and TikTok moved to block access by Russian media outlets RT and Sputnik to their platforms. Twitter begins attaching warning labels to content from Russian state media and Snapchat stops running ads on their content. ([Facebook and TikTok Restrict Russian State Media Ahead of A Likely EU Ban - Bloomberg](#); [RT, Sputnik Content Officially Banned Across European Union - Bloomberg](#))

Late February 2022 – (Approx.) CISA’s Joint Cyber Defense Collaborative (JCDC) implements a joint public-private cyber defense plan developed in December (see

entry). Eric Goldstein of CISA testifies later to a congressional subcommittee: “We exercised this plan in January, and when the invasion occurred, we moved into execution, bringing together our partners across government and the private sector to exchange information and collaborate at scale.” ([Congressional Document \(wrlc.org\)](#))

Late February 2022 – (Date approx.) Days after the Russian invasion, representatives of several large Western tech companies begin contacting Ukrainian government and private sector entities offering to help against Russian cyber intrusions. An example is Mandiant reaching out to Naftogaz, Ukraine’s largest state-owned oil and natural gas concern, a frequent target of Russian hacking attempts. A number of the Western firms are members of a group called the Cyber Defense Assistance Collaboration (CDAC), which has existed since 2009, but has not been able to marshal significant momentum toward a public-private partnership until now. *Click Here*, a production of The Record Media, posts a podcast in late November 2022 featuring first-ever in-depth interviews with some of those involved. ([EXCLUSIVE: Rounding up a cyber posse for Ukraine - The Record by Recorded Future; The Network — CDAC Network](#))

Late February – Early March 2022 – Dozens of new Telegram channels start appearing in Ukraine, mostly in occupied areas, according to Detector Media. ([«Now we will live to the fullest!». How and why Russia has created a Telegram channels network for the occupied territories of Ukraine - Детектор медиа. \(detector.media\)](#))

Spring 2022 – Following Russia’s invasion, the U.S. government ramps up its cooperation with private sector entities in a joint effort to protect Ukraine and other potential targets from Russian cyberattacks. Company executives are given security clearances to receive briefings from the NSA, USCYBERCOM, and other agencies, even foreign ones. Companies like Microsoft in turn provide intelligence from their own systems. ([Tech Companies Help Defend Ukraine Against Cyberattacks - The New York Times \(nytimes.com\)](#))

February-March 2022 – According to a Ukrainian living near Kyiv at this time and interviewed later by the *New York Times*, Russian troops entering the village make a point of destroying cellular towers and then “hunt[] people who tried to climb [to] high places” to get an internet connection. “When a close neighbor tried to climb a tree, they shot him in the leg,” the man said. ([How Russia Took Over Ukraine’s Internet in Occupied Territories - The New York Times \(nytimes.com\)](#))

February-June 2022 – According to senior Ukrainian information security official Yurri Shchylhol: “For the first four months of this invasion roughly more than 90 percent of cyberattacks were carried out against civilian sites.” ([The Man at the Center of the New Cyber World War - POLITICO](#))

Early March 2022 – In the course of early combat, Russia jams Ukrainian communications and satellite networks, cutting links between military commanders and units and

making Ukrainian drones inoperable. “Military communications were completely paralyzed,” one commander later reports. Yet, Ukrainian forces find a work-around by drawing on local citizens for intelligence. “I’m not going to put all the cards on the table, but we knew with 95 percent accuracy even their smallest movements through other means. This was all locals.” ([Battle for Kyiv: How Ukrainian forces defended and saved their capital - Washington Post](#))

Early March 2022 – After an increase in cyber operations during the first week of the invasion, Russia’s activity levels dip in the second week, then rise again in subsequent weeks, according to later comments by Mieke Eoyang, deputy assistant secretary of defense for cyber policy. ([Russia’s cyber forces ‘underperformed expectations’ in Ukraine: senior US official | The Hill](#))

Early March 2022 – Ukraine-based satellite data firm EOS Data Analytics puts out a plea for satellite data from Western companies. “We urge all global entities operating in the remote-sensing field to share recent and real-time high-to-medium resolution optical and radar satellite imagery of Ukraine and Eastern Europe with EOSDA to assist in both military and humanitarian efforts in the region.” The request adds: “We are appealing to Capella, Iceye, IQPS & Synspective, Spacety, Airbus, COSMO SkyMed, Sar-Lupe, Umbra to provide SAR data and Planet, MAXAR, Airbus, SIIS, Space View, Blacksky and other companies to provide optical data. EOSDA understands that some data providers may face certain restrictions when engaging with a private company in Ukraine. If that is the case, data suppliers will be put in touch with Mykhailo Fedorov, the Minister of Digital Transformation of Ukraine as well as other government and security officials for direct data delivery and/or sanctioning of further processing by EOSDA.” ([Satellite Data For Military And Humanitarian Aid In Ukraine \(eos.com\)](#))

March 2022 – Google’s Threat Analysis Group (TAG) later reports the following: “During our investigation into the Turla CyberAzov apps [see July 19, 2022, entry below], we identified another Android app first seen in the wild in March 2022 that also claimed to conduct DoS attacks against Russian websites. In this case, the Android app name was stopwar.apk (com.ddos.stopwar) and was distributed from the website stopwar.pro. This app is quite different from the Turla apps ... and written by a different developer.”

Google’s report adds: “Based on our analysis, we believe that the StopWar app was developed by pro-Ukrainian developers and was the inspiration for what Turla actors based their fake CyberAzov DoS app off of.” ([Continued cyber activity in Eastern Europe observed by TAG \(blog.google\)](#))

March 2022 – The Russian group Novorossia Aid Coordinating Center (NACC), founded around 2014 to back Russian actions in Ukraine, begins receiving funds, according to TRM Labs. As of early October 2022, it will have raised just over \$21,000, of which approximately 89% is in Bitcoin. ([TRM Analysis: Crypto Fundraising Groups Supporting Russian Battlefield Efforts | TRM Insights \(trmlabs.com\)](#))

March 2022 – According to TRM Labs, the Interregional Public Organization for the Promotion of the Preservation of Domestic Traditions and Cultural Heritage (MOO Veche), a Russian cultural heritage organization created in 2009, launches a Telegram channel. Between now and early October 2022, MOO Veche receives 103 deposits, totaling over \$56,000 in Bitcoin, Ethereum, Litecoin, and USDT on Tron. MOO Veche is reported to be one of several Russian-based entities tracked by TRM Labs that uses Bitcoin to raise funds to buy military equipment for various militias in Donetsk as well as Russian regular military forces. ([TRM Analysis: Crypto Fundraising Groups Supporting Russian Battlefield Efforts | TRM Insights \(trmlabs.com\)](#))

March 2022 – U.K. finance firms are targeted four times this month, the first of the year, according to data from the Financial Conduct Authority (FCA) obtained under freedom of information laws. Some analysts tie the events to Russia's invasion of Ukraine. ([DDoS Attacks on UK Firms Surge During Ukraine War - Infosecurity Magazine \(infosecurity-magazine.com\)](#))

March 2022 – The "EU Support to Strengthen Cyber Security in Ukraine" project launches. Set to run through February 2023, it is reported to be "worth" 10.7 million euros. Estonia's e-Governance Academy (eGA) is leading the effort. An article in ERR News, an arm of Estonian public broadcasting, provides details: "The project focuses on three main areas that mainly influence public service provision in Ukraine, both online and offline. Firstly, it secures [the] data exchange platform Trembita and the management of government registers, including the identification and neutralization of possible cyber threats. Secondly, it protects critical infrastructure and government data, including the replacement of destroyed hardware. Thirdly, protection equipment will be provided to enable operational staff to support and maintain critical government infrastructure." ([Estonia leading EU project to secure Ukraine's cyber, data security | News | ERR](#))

March 2022 – Ukrainian energy investor DTEK registers "a significant spike in the enemy's cyber activities" at a time when Ukrainian energy firms are actively promoting the "Stop Bloody Energy" project aimed at curtailing local purchases of Russian energy resources. ([Enemy launches hacker attacks on the power system — DTEK](#))

March 2022 – Cybersecurity experts first notice the pro-Russia hacktivist group NoName057(16) working alongside Killnet and other groups to conduct disruptive activities in Ukraine, later broadening its focus to other nations critical of Russia's invasion. ([NoName057\(16\) - The Pro-Russian Hacktivist Group Targeting NATO - SentinelOne](#))

March 2022 – A Russia-linked group, TA499, expands its campaign to embarrass high-profile critics of Russia or the war in Ukraine by posting their (reportedly "enticed") comments on YouTube or RUTUBE in order to cast them in a negative light for Russian audiences. The group has reportedly been active in this regard since at least



January 2022. ([Russian Disinformation Campaign Records High-Profile Individuals on Camera - Infosecurity Magazine \(infosecurity-magazine.com\)](#))

March 2022 – The Telegram channel of the pro-Russian hacktivist group Joker DPR is blocked, but the group immediately sets up a second one which within a year gains 247,000 subscribers. ([Joker DPR and the Information War \(recordedfuture.com\)](#))

March 2022 – The Passion group, with ties to Killnet and Anonymous Russia, appears online through Telegram. ([Passion: A Russian Botnet \(radware.com\)](#))

March 1, 2022 – Russia’s Defense Ministry warns it will target the Security Service of Ukraine (SBU) and the 72nd Center for Information and Psychological Operations (PSO) in Kyiv. “In order to thwart informational attacks against Russia, [Russian forces] will strike technological objects of the SBU and the 72nd Main PSO Center in Kiev. We urge Ukrainian citizens involved by Ukrainian nationalists in provocations against Russia, as well as Kiev residents living near relay stations, to leave their homes.” (TASS, [Russian Defense Ministry warns about strikes being prepared on military sites in Kiev - Military & Defense - TASS \(archive.org\)](#))

March 1, 2022 – The U.S. and Russian militaries establish a “deconfliction line” of communication designed to avert miscalculations and inadvertent escalations of the conflict in Ukraine. A Reuters report on November 29, 2022 (see entry), indicates it has only been used once up to that point, with no details available about the timing or circumstances. ([Russian shelling hits Ukraine power plant \(nbcnews.com\)](#); [US, Russia Agree to Deconfliction Hotline As Putin’s Attack On Ukraine Escalates - Defense One](#); [Exclusive: U.S., Russia have used their military hotline once so far during Ukraine war | Reuters](#))

March 1, 2022 – @Cyberknow20 tweets a growing list of cyberattacks targeting either Ukraine or Russia ([Cyberknow](#)):

GROUP	SUPPORTING	ATTACKS	COMMS	LOC	DATE STARTED
AgainstTheWest	Ukraine	Data Breach/Ransomware	Twitter	West Europe	2021
Belarusian Cyber Partisans	Ukraine/Free Belarus	Ransomware	Twitter	Belarus	2020
Anonymous	Ukraine	DDoS	Twitter	Global	2022
GhostSec	Ukraine	Hack	Telegram	UNK	2022
IT Army of Ukraine	Ukraine	DDoS/Hack	Twitter	Ukraine	2022
KelvinSecurity HackingTeam	Ukraine	Hack	Telegram	UNK	2022
BlackHawk	Ukraine	DDoS	Twitter	Georgia	2022
Anon Liberland & PWN-BAR	Ukraine	DDoS	Twitter	UNK	2022
RaidForums Admin	Ukraine	Sanction	Raidforums	UNK	2022
Netsec	UNK	Hack	Twitter	UNK	2022
Free Civilian	Russia	Data Breach	Onion	UNK	2022
CoomingProject	Russia	Data Breach	Onion	France	2022
Conti Ransomware Gang	Russia	Ransomware	Onion	Global	2022
The Red Bandits	Russia	Data Breach/Hack	Twitter	Russia	2022
CyberGhost	Russia	Hack/Disinformation	UNK	Belarus	UNK
SandWorm	Russia	Hack/DDoS/Disinformation	UNK	Russia	UNK
Gamaredon	Russia	Hack	UNK	Russia	UNK
28-Feb					
GNG	Ukraine	DDoS	Twitter	Georgia	2022
NB65	Ukraine	Hack	Twitter	UNK	2022
ECO	UNK	UNK	Twitter	UNK	2022
RaidForums2	Ukraine	DDoS	Twitter	UNK	2022
ContiLeaks	Ukraine	Data Breach	Twitter	UNK	2022
SHDWSec	Ukraine	Hack/Activism	Twitter	Global	2022
GhostClan	Ukraine	Hack/DDoS	Telegram	Global	2022
Eye of the Storm	Ukraine/Free Belarus	Hack	Twitter	Global	2022
1-Mar					
Root User	Ukraine	Radio	Twitter	Ukraine	2022
DeepNetAnon	Ukraine	Radio	Twitter	UNK	2022
FreeUkraineNow	Ukraine	DDoS/Hack	Twitter	Ukraine	2022
1LevelCrew	Ukraine	DDoS	Twitter	UNK	2022
IT Army of Ukraine Psyps	Ukraine	Disinformation	Twitter	Ukraine	2022
Hydra UG	Ukraine	Radio/data breach	Twitter	UNK	2022
Zatoichi	Russia	Disinformation	Twitter	Russia	2022
Stormous Ransomware	Russia	Ransomware	Telegram	UNK	2022

March 1, 2022 – Microsoft later reports: “Kyiv-based media companies face destructive attacks and data exfiltration.” ([An overview of Russia’s cyberattack activity in Ukraine \(microsoft.com\)](#))

March 1, 2022 – A Kyiv-based security firm, Cyber Unit Technologies puts out an offer to legitimate white hat hackers to join a campaign to target Russian websites. The company pledges \$100,000 to be used as part of the reward. ([This Ukrainian cyber firm is offering hackers bounties for taking down Russian sites - The Record by Recorded Future](#))

March 1, 2022 – @YourAnonTV tweets that “Hacking group ‘NB65’ ... has shut down the Control Center of the Russian Space Agency ‘Roscosmos.’ #Russia has no more control over their own Spy-Satelites.” Roscosmos head Dmitry Rogozin quickly denies the report, adding the warning: “Offlining the satellites of any country is actually a casus belli, a cause for war.” *Politico* later notes that “military officials have long seen the cyber threat to military and civilian space systems as another front; the U.S. Space Force, for example, warned last year that satellites get hacked on nearly a daily basis. ‘That’s probably one of the biggest potential exposed flanks,’ according to Col. Benjamin Ogden, space operations officer at the Army War College, quoted by *Politico*. ([Twitter](#); [Russia space agency head says satellite hacking would justify war -report | Reuters](#); [Russia's space chief says hacking satellites 'a cause for war' - POLITICO](#))

March 1, 2022 – Ukraine's *Pravda* newspaper prints what purports to be personal data on 120,000 Russian troops fighting in Ukraine. Cyber expert Thomas Rid tweets: "[I]f confirmed as accurate, we're probably looking at one of the best-timed and most devastating leaks of all time." But he adds: "Important to note that there's a long history of leaking lists of names of covert personnel ... We have examples of lists that are entirely legit, and some that were at least in part forged, for practical and psychological effect." ([Особисті дані 120 тисяч військових РФ, що воюють в Україні – ЦОС | Українська правда \(pravda.com.ua\)](#); [Twitter](#))

March 1, 2022 – MalwareHunterTeam tweets about the discovery of a possible ransomware variant. Its developer calls it "RURansom." A week later, Trend Micro reports finding several more samples of the malware but says it is a wiper and not a ransomware variant "because of its irreversible destruction of encrypted files. Based on our telemetry, we have not yet observed active targets for this malware family. One possible reason for this is that the wiper has only targeted a few entries in Russia so far. RURansom's code, however, makes its author's motives clear." An unedited translation from Russian of a note in the code reads: "On February 24, President Vladimir Putin declared war on Ukraine.", "To counter this, I, the creator of RU\_Ransom, created this malware to harm Russia. You bought this for yourself, Mr. President.", "There is no way to decrypt your files. No payment, only damage. And yes, this is \"peacekeeping\" ..." ([New RURansom Wiper Targets Russia \(trendmicro.com\)](#))

"This is very rare to see the ransomware that targets Russia specifically," according to Lotem Finkelstein of the Israeli cybersecurity company Check Point. *Wired* notes that the marked increase in attacks on Russian systems may encourage the country to isolate itself further in cyberspace. ([Russia Is Being Hacked at an Unprecedented Scale | WIRED](#))

March 2, 2022 – The European Union bans Russian media outlets Russia Today (RT) and Sputnik. High Representative and Vice-President Josep Borrell explains in a statement: "Systematic information manipulation and disinformation by the Kremlin is applied as an operational tool in its assault on Ukraine. It is also a significant and direct threat to the Union's public order and security. Today, we are taking an important step against Putin's manipulation operation and turning off the tap for Russian state-controlled media in the EU. We have already earlier put sanctions on leadership of RT, including the editor-in-chief Simonyan, and it is only logical to also target the activities the organisations have been conducting within our Union."

On February 27, Commission President Ursula von der Leyen announced the organization would soon take the "unprecedented step" of blocking "the Kremlin's media machine" and was already "developing tools to ban their toxic and harmful disinformation in Europe." ([Ukraine: Sanctions on Kremlin-backed outlets \(europa.eu\)](#))

March 2-4, 2022 – The pro-Russian hacktivist groups Killnet and Xaknet begin to claim responsibility for various DDoS attacks. ([Dark Covenant 2.0: Cybercrime, the Russian State, and the War in Ukraine \(recordedfuture.com\)](#))

March 2, 2022 – Microsoft later reports: a “Russian group moves laterally on network of Ukrainian nuclear power company.” ([An overview of Russia’s cyberattack activity in Ukraine \(microsoft.com\)](#))

March 2, 2022 – A *Lawfare* article calling for a “cyber realism in a time of war” discusses the surprising lack of serious cyberattacks by either Russia or Ukraine, beyond essentially attempts to harass and embarrass. Author Ciaran Martin goes on to assess the ongoing cyber threat to the West, what actual cyber capabilities consist of, what limitations they face, and what the implications are for Western planners. He concludes that “the cyber domain may influence the war at the margins, but it will not decide it.” ([Cyber Realism in a Time of War - Lawfare \(lawfareblog.com\)](#))

March 2, 2022 – *Time* publishes a broad overview of “Why Russia Hasn’t Launched Major Cyber Attacks Since the Invasion of Ukraine.” The article notes that “as the invasion continues with few signs of any sophisticated cyber conflict, it seems less and less likely that Russia has significant cyber capabilities in reserve, ready to deploy if needed. Instead, it begins to look like Russia’s much vaunted cyber capabilities have been neglected in recent years, in favor of developing less expensive, less effective cyber weapons that cause less widespread damage and are considerably easier to contain and defend against.” The piece adds that while outside help from governments and companies like Microsoft “has undoubtedly helped curb the damage ... if Russia really had on hand a stockpile of previously undetected vulnerabilities and sophisticated malware designed to exploit them, these lines of defense simply would not be enough to prevent some significant damage and disruption.” ([Why Russia Hasn’t Launched Major Cyber Attacks | Time](#))

March 3, 2022 – With an eye to sowing confusion and unrest, according to a Ukrainian cyber official, hackers post calls to surrender on local community websites in the Odessa region along with disinformation about the Snake Island attack. (Dmytro Dubov, “Russia’s in Ukraine: The War in Cyberspace” (Series No. 2)

March 3, 2022 – The Biden administration submits a request to Congress for \$10 billion in emergency humanitarian and defense aid for Ukraine. This is almost \$4 billion above the White House’s preliminary request. Among the purposes is to provide a boost in intelligence and cybersecurity support. ([What Happened on Day 8 of Russia’s Invasion of Ukraine - The New York Times \(nytimes.com\)](#))

March 3, 2022 – The *Washington Post*’s Cybersecurity 202 lists 11 reasons (with commentary from experts) why Russia has not yet hit Ukraine with a full cyber offensive.

- They’re keeping the good stuff in reserve



- Big hacks are happening that we just don't know about
  - Russian hackers weren't prepared for the invasion
  - Russia didn't think big cyberattacks were necessary
  - Major cyberattacks just aren't that useful during a shooting war
  - Fear of escalating cyber tensions with the West
  - Russia wants to keep Ukraine's infrastructure intact for a future occupation
  - Ukraine's cyber defenses are working
  - Global cyber defenders have blunted the worst Russian hacks
  - Russia's best hackers are busy spying
  - Kremlin hackers' hearts just aren't in the fight
- ([11 reasons we haven't seen big Russian cyberattacks yet - The Washington Post](#))

March 3, 2022 – Cybersecurity provider Trustwave reports observing a “high volume of cyber activity on the Dark Web” aimed at influencing the Ukraine war. Most activities to date differ from previous geopolitical conflicts where hackers “tended to be less destructive” and more interested in “public perception.” Still, the group finds that most of the detected efforts do not seem to be connected to either the Russian or Ukrainian governments. ([Dark Web Insights: Evolving Cyber Tactics Aim to Impact the Russia-Ukraine Conflict | Trustwave](#))

Early March - Victor Zhora, deputy chairman and chief digital transformation officer at the State Service of Special Communications and Information Protection in Ukraine, tells a press conference that the Viasat attack of February 24 caused a “really huge loss in communications,” but he does not provide details. In sept 2022, Zhora walks back the comments, calling them a misunderstanding. (See September 26, 2022, entry) ([Viasat Hack "Did Not" Have Huge Impact on Ukrainian Military Communications. Official Says \(substack.com\)](#))

March 4, 2022 – NATO's Cooperative Cyber Defence Centre of Excellence (CCDCOE), a key component of the alliance's cybersecurity approach, accepts Ukraine as a contributing participant following a unanimous vote by the 27-member Steering Committee. ([CCDCOE; Ukraine to join NATO CCDCOE \(janes.com\)](#))

March 4, 2022 – Russia's parliament adopts two laws that criminalize the use of what the government terms “false information” aimed at “discrediting” the armed forces as well as “public actions” taken with the same intent, e.g. public protests calling for an end to the war. The new laws, which Parliament on March 23 amends to broaden their scope (to cover basically all Russian government entities and actions abroad), are seen as largely aimed at stifling unfriendly news coverage as well as public dissent. ([Russia Criminalizes Independent War Reporting, Anti-War Protests | Human Rights Watch \(hrw.org\)](#))

March 4, 2022 – A new Twitter account, @trickleaks, appears and tweets the following: “We have evidence of the FSB's cooperation with members of the Trickbot criminal group (Wizard Spider, Maze, Conti, Diavol, Ruyk).” This is followed by tweets with

links to internal messages from the Trickbot group, which has roughly 1,700 followers. Over the next two months, a total of more than 1000 communication extracts are leaked.

According to the British cybersecurity firm Cyjax: “Each file consists of a direct communication or a group chat involving the user, which range in size. Some files contain nearly 10,000 messages. In total, there are approximately 250,000 messages which contain over 2,500 IP addresses, around 500 potential crypto wallet addresses, and thousands of domains and email addresses.”

Cyjax continues: “This leak was like nothing seen before and gave cyber threat intelligence researchers unprecedented access to the Trickbot organisation. To put this leak into perspective, it was over four times the size of the Conti leaks which was seen by some researchers as one of the most useful information dumps of the past few years. Alongside these messages, PDF files were leaked which contained large amounts of information reportedly about individual members. This included full names, addresses and identification numbers. These “Doxing PDF” files have given us the ability to analyse the people behind the usernames, examining how and why they are working for the criminal organisation.” ([Who is Trickbot? ★ Cyjax](#))

March 4, 2022 – The GRU-linked group STRONTIUM compromises a government network in Vinnytsia, according to a later Microsoft report. ([An overview of Russia's cyberattack activity in Ukraine \(microsoft.com\)](#))

March 4, 2022 – Amazon posts a blog saying: “For several weeks, we have been partnering closely with Ukrainian IT organizations to fend off attacks and working with organizations in Ukraine, and around the world, to share real-time, relevant intelligence. As a result, our teams have seen new malware signatures and activity from a number of state actors we monitor. As this activity has ramped up, our teams and technologies detected the threats, learned the patterns, and placed remediation tools directly into the hands of customers ... Our security teams are sharing this intelligence with governments and IT organizations that we partner closely with from Europe, North America, and around the world ....

“While we are seeing an increase in activity of malicious state actors, we are also seeing a higher operational tempo by other malicious actors. We have seen several situations where malware has been specifically targeted at charities, NGOs, and other aid organizations in order to spread confusion and cause disruption. In these particularly egregious cases, malware has been targeted at disrupting medical supplies, food, and clothing relief.” ([Amazon's cybersecurity assistance for Ukraine \(aboutamazon.com\)](#))

Early March 2022 – An organization called Distributed Denial of Secrets (DDoSecrets) posts links to more than 360,000 leaked files (over 817GB) from Roskomnadzor, the Russian Federal Service for Supervision of Communications, which oversees Russians' access to and use of the Internet, among other roles. The source of the leak is not named but the site indicates they denied any connection to the federal agency.

(For assessments of the leaked materials, see April 13 and September 22, 2022, entries.) ([Roskomnadzor - Distributed Denial of Secrets \(ddosecrets.com\)](https://ddosecrets.com/))

March 7, 2022 – Google’s Threat Analysis Group (TAG) posts an update describing some of the recent activity of several threat actors. Fancy Bear/APT28 is attributed to the GRU and has been targeting Ukrainian users of UkrNet, a media company with phishing emails. Ghostwriter/UNC1151 is described as a Belarusian entity that in the past week has been targeting Polish and Ukrainian government and military organizations. Mustang Panda or Temp.Hex is based in China and has been attaching zip files with names relating to the Ukraine crisis as a lure to get European users to open them. ([An update on the threat landscape \(blog.google\)](https://blog.google.com/threat-analysis-group/))

March 8, 2022 – The heads of the main U.S. intelligence agencies testify before the House Intelligence Committee on global threats, including numerous remarks on Ukraine and on cyber. Gen. Paul Nakasone says that his agency is focusing on three main types of Russian activity: ransomware, scenario proxies by non-nation-state actors, and disruptive/destructive attacks.

Asked by Rep. Jackie Speier (D-CA) why Russia has not engaged in heavy cyber activities to date in Ukraine, Gen. Paul Nakasone replies: “... In terms of Russia, they have conducted several attacks in the Ukraine, three or four upon which we have watched and we have tracked very carefully. In terms of why they haven't done more, I think that that is obviously some of the work that the Ukrainians have done, some of the challenges that the Russians have encountered, and some of the work that others have been able to prevent their actions. And so it has not been what we would anticipate when we were going into this several weeks ago.”

Nakasone and FBI Director Christopher Wray discuss the importance of cyber alliances:

Nakasone: “So, Congressman, I think that what you hit on is really the key for the future of these series of partnerships that we have. And we have seen the partnerships. I sit next to Director Wray, who has been a tremendous partner in our ability to get after some of the cybersecurity threats here in our Nation. But it is broader than that, as you had indicated. So we have rich partnerships with obviously our FBIS partners and series of other partners within both Europe and the Pacific. And as far as the work that we do full spectrum, I would like to take that on this afternoon because I think that would be appropriate, given the discussions we have had this morning on Russia and the Ukraine.” [...]

Wray: “I would just add – completely agree with General Nakasone – but I would add that just about every significant major takedown that we have engineered together against foreign adversaries, cyber adversaries, whether they be criminal or nation-state, almost invariably involved a whole slew of foreign partners all acting in concert. And one of the clear lessons from the last few years is that that is the most effective weapon against cyber adversaries is joint sequenced operations. I like to say cyber is sort of the ultimate team sport, and we do that with our foreign partners.” ([IG067001 \(house.gov\)](https://www.house.gov/legislation/record/hrg067001.htm))

March 8, 2022 – *Politico* publishes an in-depth interview with Oleksandr “Alex” Bornyakov, Ukraine’s deputy minister of digital transformation. Bornyakov describes the country’s cyber campaign using, among other things, the so-called IT Army of Ukraine. “We are the first in the world to introduce this new warfare. And it’s powerful, yet simple at the same time ... It’s impossible to disrupt it or break it down.” He also discusses using cryptocurrencies to raise money. “I like the global financial and banking systems. I use Apple Pay and everything like that. But in wartime, you have to make decisions very fast, and crypto allows us to avoid waiting days for bank transfers. So, you can immediately use the funds ... We have several funds now.” Those funds currently are worth \$65 to \$70 million. ([‘We Are the First in the World to Introduce This New Warfare’: Ukraine’s Digital Battle Against Russia - POLITICO](#))

March 8, 2022 – A detailed *Wired* article analyzes leaked messages and files from the Conti group to assess its apparent support for Kremlin policies. The piece concludes: “Members of the hacker gang may act in Russia’s interest, but their links to the FSB and Cozy Bear hackers appear ad hoc.” In one April 2021 exchange, Mango, a Conti manager, asks another senior group member called Professor: “Do we work on politics?” Later, Mango asks: “I mean, are we patriots or what?” “Of course we are patriots,” Professor replies. ([Conti Leaks Reveal the Ransomware Group’s Links to Russia | WIRED](#))

March 9, 2022 – Ukrainian telecom provider Triolan is the target of a cyberattack. (Cyber Peace Institute, “Ukraine: Timeline of Cyberattacks...,” cited in [Lin-Russian Cyber Operations in Ukraine-Cyber Defense Review-2022-fall.pdf](#))

March 9, 2022 – Microsoft alerts the U.S. government about their discovery of destructive malware on Ukrainian networks, according to Anne Neuberger, deputy national security advisor for cyber and emerging technology, later. ([Opinion | How Far Would Biden Go in a Cyberwar Against Putin? - The New York Times \(nytimes.com\)](#))

March 9, 2022 – NATO Secretary General Jens Stoltenberg delivers a speech at the Ottawa Conference on Security and Defence in which he declares “Russia has shattered peace in Europe ... President Putin’s war is not only against international law, it seeks to destroy the entire international rules-based order.” In a follow-up discussion, Stoltenberg replies to a question about Russian cyber and disinformation activity:

“Well, cyber is, will be and is, a part of any military confrontation, there will be a cyber dimension. And of course, we are faced with this more blurred line between peace and war, hybrid tools, hybrid conflicts. And of course, Allies have reported about many different types of cyberattacks against political institutions, private companies. We have seen attempts to meddling in political, domestic, democratic processes in different countries, and attributed this to Russia in many of the cases.

“So NATO has significantly stepped up the way we address cyber threats. We have, as you alluded to, also decided to make clear that a cyberattack can trigger



Article 5. But we will never give the privilege to a potential adversary to tell exactly where that threshold is. But we will deem, we will assess, and then we will make our own decisions when we trigger Article 5.

“Then, of course, we can respond in cyber. But we can also respond in another domain. We have established now cyber as a military domain alongside, air, sea, land and... space. And, for instance, for Ukraine we have, over the years but also recently, help them to improve their cyber defences, to protect their own networks. We recently signed the agreement with Ukraine on how to facilitate, support. That was before the invasion but Allies and NATO are helping with cyber defences. And because this is so important for Ukraine, but also for all NATO Allied countries.”

[\(NATO - Opinion: Speech by NATO Secretary General Jens Stoltenberg at the Ottawa Conference on Security and Defence, 09-Mar.-2022\)](#)

March 10, 2022 – Russia's Defense Ministry claims it has uncovered “U.S. secret military biological projects in Ukraine,” according to state-run media. The next day, Russia's U.N. mission in New York calls for an emergency meeting of the Security Council. Western governments dismiss the claim as part of the Kremlin's disinformation campaign. ([Russia escalates false chemical weapons claims about US, Ukraine by bringing them to UN - ABC News \(go.com\)](#))

March 10, 2022 – DNI Avril Haines and Gen. Paul Nakasone speak approvingly about new approaches to intelligence sharing during testimony before the Senate Intelligence Committee. Senator Angus King (I-ME) notes: “It appears that a conscious decision was made to share more. Is that the case?”

Haines: “Yes, we have – all of us – I think engaged in this and it has been an extraordinary team effort, to be honest, in trying to promote more mechanisms for sharing, finding ways to make sure that we're integrating our work across the Intelligence Community and providing that information to partners and allies in this context, and also disclosing certain things publicly, as you've indicated. And I think it really has been, at least from my perspective, critical to the diplomatic effort. I think it has helped to galvanize the response and also, I hope, helped to prepare the Ukrainians to some extent [...]

Nakasone: [...] “We share a lot of intelligence but here's the difference: the intelligence that we're sharing is accurate, it's relevant, and it's actionable I think when we look back at this that's the key piece of what we've been able to do as an intelligence community.”

Sen Ben Sasse (R-NE) asks: “General Nakasone, you all have done some really great work sharing intelligence to expose what Putin was up to. What do you think the implications will be one or two or three years from now, from what we've learned from this more aggressive promiscuous helpfully promiscuous sharing of Intel in advance?”

Nakasone: “I think we'll redefine sharing, Senator. You talk about sharing with our partners ... [the] impact on bringing a coalition together. We talk about sharing with the Ukrainians, actionable intelligence that allows them to be able to take combat operations to a new level. I think that the other piece is being able to shine a light on disinformation. We've seen this in the elections – 2018, 2020, when

we take out an adversary, when we work with a series of partners – to be able to shine a light on these missed stories and these false flag operations. It suddenly isn't as big a deal and I think that's what we'll learn from sharing." ([SSCI Transcript 10 March 2022.docx \(cia.gov\)](#))

March 10, 2022 – Also during their testimony before the Senate Intelligence Committee, DNI Avril Haines and DIA head Lt. Gen. Scott Berrier acknowledge initial miscalculations regarding Ukraine and Russia. Berrier admits: "My view was that, based on a variety of factors, that the Ukrainians were not as ready as I thought they -- as I thought they should be. Therefore, I -- I questioned their will to fight. That was a bad -- that was a bad assessment on my part, because they have fought bravely and honorably and are -- are doing the right thing. So, that -- that was an issue for -- for me as the director of DI." Haines says that while Vladimir Putin underestimated the Ukrainians, so did U.S. intelligence: "We did not do as well in terms of predicting the military challenges that he has encountered with his own military." ([SSCI Transcript 10 March 2022.docx \(cia.gov\)](#))

March 10, 2022 – During a wide-ranging interview on the podcast "Sway," Anne Neuberger, deputy national security advisor for cyber and emerging technology, discusses how U.S. strategists have looked at ways the Ukraine war could unfold. "So the three scenarios we've used in our both internal government discussions and discussions with our colleagues at NATO with the European Union and certainly with our Ukrainian colleagues has been first a potential disruptive attack against Ukraine. And how do we virtually ensure that we can provide incident response support to recover services quickly? The second would be a scenario akin to what we saw with NotPetya in 2017, where a Russian cyber attack against Ukraine spread and ended up having billions of dollars of impact around the world. And then finally, a potential disruptive attack against our European colleagues or the U.S. in response to sanctions."

Neuberger continues: "And we use those [scenarios] to exercise really our three-part strategy, which is first above all, hardened systems. Because at their root, technology is full of vulnerabilities. And those are the ones that less capable all the way through to really capable actors leverage. Second, warn. Let's create a sense of urgency in the private sector to do the kinds of things that do have impact — locking digital doors, putting on a digital alarm system. And then finally, ensure that we make it harder for attackers to conduct disruptive operations, whether that is disrupting infrastructure and more sensitive operations that I won't get into here. But that three-part strategy, we've been exercising it regularly against the scenarios we've talked about to ensure we're as prepared as we can be." ([Opinion | How Far Would Biden Go in a Cyberwar Against Putin? - The New York Times \(nytimes.com\)](#))

March 10, 2022 – Palantir CEO Alexander Karp calls on Europe, in the wake of the Ukraine war, to step up and "become a leader in disruptive defense technology." He argues that "The soft power and cultural influence that many in Europe and the United States had hoped would someday make militaries obsolete has failed spectacularly to stem the aspirations of autocratic rule." "The continent certainly understands that

its defense and that of its allies now requires the development of an indigenous source of strength and capacity to defend itself, and quickly.” In addition, he points up the need for ties between government and industry. Recalling the factors that enabled the rise of high tech in the United States, he notes that “the founding spark for Silicon Valley was its embrace of the defense objectives and technological aims of the government whose very existence made its rise possible .... Our expansion as a company over the years was made possible by our work with government agencies in the military and intelligence sectors in the United States, whose leaders took an interest in software and understood its potential to reshape national defense. Software as much as anything else is a product of the legal and moral order from which it stems and plays a role in defending it.” For Europe, the same kind of shift will require an equivalent “embrace of the relationship between technology and the state.” (Karp open letter, “In Defense of Europe,” 3-10-22)

March 10, 2022 – A Wikipedia editor based in Belarus, Mark Bernstein, is doxxed and later arrested and detained in Minsk, eventually receiving a three-year sentence of restricted freedom for “activities that disrupt social order.” The same month, at least four other Wikipedia editors from Russia and elsewhere in the region are doxxed in what some observers see as part of a larger program by Moscow and its allies to suppress the platform because of negative portrayals of the Ukraine war. ([Doxxed, threatened, and arrested: Russia’s war on Wikipedia editors - Rest of World](#))

March 10, 2022 – The White House hosts 30 TikTok influencers for a Zoom call on the war in Ukraine. NSC special adviser for communications Matt Miller and Press Secretary Jen Psaki meet with the group. The meeting is an acknowledgement of the impact of TikTok as an information source for millions of users. ([Stream episode White House Press Briefing TikTokers Ukraine by taylorlorenz podcast | Listen online for free on SoundCloud](#); [INSIDE The White House’s Briefing with TikTok Creators | Breaking Points with Krystal and Saagar - YouTube](#); [TikTok stars receive White House briefing on Ukraine - The Washington Post](#))

March 11, 2022 – Microsoft later reports: a “Dnipro government agency [is] targeted with [a] destructive implant” on the same day the first Russian strikes in Dnipro hit government buildings. ([An overview of Russia’s cyberattack activity in Ukraine \(microsoft.com\)](#))

March 12, 2022 – A detailed article by Kim Zetter in *Politico* discusses the issues surrounding U.S. and Russian calculations over whether, when, and to what extent to initiate a direct cyber conflict. Several former cyber professionals agree neither side will move swiftly to attack targets such as critical infrastructure, largely out of uncertainty over how powerfully their adversary might respond. ([‘Not the time to go poking around’: How former U.S. hackers view dealing with Russia - POLITICO](#))

March 13, 2022 – Ukrainian telecom provider Vinasterisk is the target of a cyberattack. (Cyber Peace Institute, “Ukraine: Timeline of Cyberattacks...,” cited in [Lin-Russian Cyber Operations in Ukraine-Cyber Defense Review-2022-fall.pdf](#))

March 13, 2022 – Microsoft: “On March 13, a suspected Russian nation state actor stole data from a nuclear safety organization that FSB-affiliated actor BROMINE had compromised in December 2021. BROMINE stole data from this entity from December through mid-March.” ([An overview of Russia’s cyberattack activity in Ukraine \(microsoft.com\)](#))

March 14, 2022 – Air Force Brig. Gen. Chad D. Raduege, chief information officer of U.S. European Command, tells a public audience the U.S. military does not have adequate cyber defense resources to accomplish an ever-widening mission. “There’s been a realization that, quite frankly, we can’t protect everything we have.” Speaking about his experiences in 2021 with Air Combat Command, he noted there was “a really great vision” aimed at protecting weapons systems and other objectives. “What we found is we didn’t have enough capacity in the cyber realm to even stand up some of those capabilities.” Currently, he says, the “demand signal” for cyber protection is being propelled the U.S. response to the Ukraine war, which involves a wide range of players and missions, all demanding connectivity. ([Cyber Troops Stretched Thin in Ukraine Response as NATO Builds Common Air Picture - Air Force Magazine](#))

During congressional testimony the following month, USCYBERCOM head Nakasone gives his reaction: “So, we can talk about this in more detail in the closed session. But what I would offer here is that one of the very big lessons that we’ve learned is the ability to deploy a number of different teams early on in a crisis to US European Command, and then working with General Wolters and his staff, making sure that those experts, those teams go to the places that are necessary.” ([Congressional Document \(wrlc.org\)](#))

March 15, 2022 – Ukraine discovers the existence of new malware called Caddy Wiper. ([Telegram: Contact @dsszzi official](#))

March 15, 2022 – CISA and the FBI send out an alert “to warn organizations that Russian state-sponsored cyber actors have gained network access through exploitation of default MFA [multifactor authentication] protocols and a known vulnerability.” The alert notes that these actors earlier exploited a critical Windows Print Spooler vulnerability known as “PrintNightmare” at an unnamed NGO. ([Russian State-Sponsored Cyber Actors Gain Network Access by Exploiting Default Multifactor Authentication Protocols and “PrintNightmare” Vulnerability | CISA](#))

March 16, 2022 – The Ukrainian information protection agency reports that as of this date more than 3,000 attacks including “phishing mailing, dissemination of malicious software and DDoS” have taken place. (Ukrainian official statement, [Since February 15, Ukraine has suffered over 3000 DDoS attacks \(cip.gov.ua\)](#), 3-16-22)

March 16, 2022 – The *New York Times* reports that “many Russian generals are talking on unsecured phones and radios. In at least one instance,” according to two American military officials, “the Ukrainians intercepted a general’s call, geolocated it, and



attacked his location, killing him and his staff.” ([As Russian Troop Deaths Climb, Morale May Be an Issue - The New York Times \(nytimes.com\)](#))

March 16, 2022 – A news article discusses how Telegram has sustained its popularity in Ukraine and Russia amid the war, becoming a “lifeline” as an early warning device and survival guide for Ukrainians. This is despite concerns about its security shortcomings. The article quotes Signal creator Moxie Marlinspike warning that Telegram is not an “encrypted app.” ([How Telegram found itself in the middle of the war between Russia and Ukraine - The Record by Recorded Future](#))

March 16-17, 2022 – In “the most notable mass cyber-campaign of Russia’s war in Ukraine” to date, writes Ukrainian cyber official Dmytro Dubov, over a dozen Ukrainian information resources have been targeted. The on-air news feed of TV channel Ukraine 24 is the main focus, centered around the launch of a rumor that Ukraine was surrendering and an “extremely low-quality deepfake” on social media of an alleged speech to that effect by President Zelensky. Hackers have also homed in on a large number of Ukrainian media websites and tried to post “Z” and other Russian banners on 10+ sites. (Dmytro Dubov, “Russia’s in Ukraine: The War in Cyberspace” (Series No. 2))

March 17, 2022 – Hackers post fake propaganda on the Ukrainian judiciary website alleging so-called Ukrainian “nationalists” have been using civilians as human shields. (Dmytro Dubov, “Russia’s in Ukraine: The War in Cyberspace” (Series No. 2))

March 17, 2022 – The European Union Aviation Safety Agency issues a Safety Information Bulletin that states: “In the current context of the Russian invasion of Ukraine, the issue of Global Navigation Satellite Systems (GNSS) jamming and/or possible spoofing has intensified in geographical areas surrounding the conflict zone and other areas.” The bulletin lists several areas in particular along with a number of recommendations. ([EASA Safety Publications Tool \(europa.eu\)](#))

March 17, 2022 – Director of the Defense Intelligence Agency Army Lt. Gen. Scott Berrier tells the House Armed Services Committee the level of intelligence sharing with Ukraine has been “revolutionary in terms of what we can do.” USCYBERCOM Commander and NSA Director Army Gen. Paul Nakasone adds that he has never seen a better example “in my 35 years in uniform.” They defer details to a closed session. ([Intel Sharing Between U.S. and Ukraine 'Revolutionary' Says DIA Director - USNI News; https://youtu.be/sr54QBU2lBc](#))

March 17-23, 2022 – At some point during this week, according to Microsoft, GRU affiliate IRIDIUM “conducted a destructive attack on the network of a transportation/logistics provider, the type of organization that could be involved in moving Ukrainian supplies to conflict hotspots. The firm is headquartered in Western Ukraine, where much of the foreign military and humanitarian assistance is entering the country.” ([An overview of Russia’s cyberattack activity in Ukraine \(microsoft.com\)](#))

March 18, 2022 – After obtaining a court order, a range of U.S. government agencies and bureaus conduct an operation to “disrupt a two-tiered global botnet” run by Russia’s GRU. The botnet consisted of “thousands of infected network hardware devices under the control of a threat actor known to security researchers as Sandworm,” attributed to the GRU. The operation involved “working closely with WatchGuard and other government agencies in this country and the United Kingdom to analyze the malware and to develop detection and remediation tools.” The news release touts this as an example of the “strength that public-private partnership brings to our country’s cybersecurity.” Government entities participating in the operation include: the FBI’s Pittsburgh, Atlanta and Oklahoma City Field Offices; the FBI Cyber Division; the National Security Division’s Counterintelligence and Export Control Section; the U.S. Attorney’s Office for the Western District of Pennsylvania; the DOJ Criminal Division’s Computer Crime and Intellectual Property Section and Office of International Affairs; and the U.S. Attorney’s Office for the Eastern District of California. (DOJ release, 4-6-22)

March 18, 2022 – “Chinese authorities are almost certainly watching and learning from Russia’s ongoing war in Ukraine and any accompanying cyber activity,” Analyst Zoe Haver writes in Recorded Future. Haver has uncovered procurement documents and other evidence that government entities, state-owned enterprises, and PLA-linked organizations have paid specific attention to events such as the December 2015 attack on Ukraine’s power grid (see December 23, 2015, entry above). ([China’s Government Is Learning From Russia’s Cyberattacks Against Ukraine \(recordedfuture.com\)](https://www.recordedfuture.com/china-government-learning-russia-cyberattacks-ukraine))

March 19, 2022 – An attempted attack on Ukraine’s power grid reportedly takes place and CERT-UA describes it as “successful” in a document later shared with MIT Technology Review, among others. The document states that nine electric substations were temporarily shut down. But Viktor Zhora, deputy head of the State Special Service for Digital Development, says later that report was “preliminary” and he subsequently called it a “mistake.” ([Russian hackers tried to bring down Ukraine's power grid to help the invasion | MIT Technology Review](https://www.mitre.org/news/ukraine-power-grid))

March 20, 2022 – An unidentified source leaks more of Conti’s internal source code (though it is password protected). It is at least the fourth such disclosure. ([More Conti ransomware source code leaked on Twitter out of revenge \(bleepingcomputer.com\)](https://www.bleepingcomputer.com/news/conti-ransomware-source-code-leaked-on-twitter-out-of-revenge))

March 20, 2022 – The *Wall Street Journal* describes the impact of the Ukraine war on efforts of local companies to protect employees and their operations. “In an escalating war, business leaders responsible for large Ukrainian workforces have become evacuation coordinators, military strategists, providers of humanitarian aid and, in some cases, financiers of the Ukrainian army .... Their preparations for the war started months ago. The startups secured passports and Covid-19 vaccines for employees and their families, converted money into U.S. dollars and transferred

staff to safer locales. Now, from perches in Poland, Germany, Israel, Silicon Valley and elsewhere, these startup leaders continue to run their businesses while adding another task—helping to defend Ukraine.” ([Ukraine Tech Startups Pivot From Software Code to Rescue Plans - WSJ](#))

March 21, 2022 – President Biden issues a renewed public warning about the potential for malicious Russian cyber activity. ([Statement by President Biden on our Nation’s Cybersecurity | The White House](#))

March 21, 2022 – A Moscow court rules that Meta has been carrying on extremist behavior which effectively prohibits Facebook and Instagram from operating in the country. But the court specifically excludes WhatsApp from the prohibition. Speculation centers around the latter’s popularity with many ordinary Russians whom the Kremlin does not want to alienate. ([Why WhatsApp Survived Russia’s Social Media Purge | WIRED UK](#))

March 22, 2022 – SpaceX President Gwynne Shotwell tells CNBC the company has sent “thousands” of Starlink satellite kits to Ukraine since the invasion. The kits use satellites to enable internet connections that evade government blocking attempts. Shotwell indicates most of the funding has been private but that France and perhaps Poland have “helped.” ([Elon Musk’s SpaceX sent Ukraine thousands of Starlink satellite dishes, exec says \(cnbc.com\)](#))

A later CNN story reports that Ukrainian bought a block of 1,300 terminals sometime in March from a British company for combat-related operations. Those terminals suddenly go offline starting on October 24 (see entry), reportedly due to Ukraine’s inability to pay the \$2,500 per month SpaceX charges to keep each terminal connected. ([Ukraine suffered a comms outage when 1,300 SpaceX satellite units went offline over funding issues | CNN Politics](#))

March 23, 2022 – Anonymous tweets that the group has hacked Russia’s Central Bank and will expose 35,000 files in the next 48 hours. The bank is a key institution especially in formulating Russia’s monetary policies. ([\(9\) Anonymous on Twitter](#))

March 24, 2022 – The Justice Department indicts four Russian nationals “who worked for the Russian government, with attempting, supporting and conducting computer intrusions that together, in two separate conspiracies, targeted the global energy sector between 2012 and 2018. In total, these hacking campaigns targeted thousands of computers, at hundreds of companies and organizations, in approximately 135 countries.” ([Four Russian Government Employees Charged in Two Historical Hacking Campaigns Targeting Critical Infrastructure Worldwide | OPA | Department of Justice](#))

March 24, 2022 – CISA, FBI, and DOE send out a joint Cybersecurity Advisory (CSA) providing details about “multiple intrusion campaigns conducted by state-sponsored Russian cyber actors from 2011 to 2018 and targeted U.S. and

international Energy Sector organizations.” ([Tactics, Techniques, and Procedures of Indicted State-Sponsored Russian Cyber Actors Targeting the Energy Sector | CISA](#))

March 24, 2022 – Top NATO political leaders meet in Brussels. Discussing the impact of Russia’s invasion of Ukraine, Secretary-General Jens Stoltenberg says it has changed the global security environment and requires a continuing strong response. Among other areas of expanded military support, he adds, the alliance “will also strengthen our cyber defenses.” ([NATO Leaders Discuss Responses to Russia's Ukraine Invasion > U.S. Department of Defense > Defense Department News](#))

March 24-30, 2022 – According to Microsoft, “Unknown actors compromised and potentially destroyed data at a portal that connects [Ukrainian] citizens to government services and compromised the network of another major media organization.” ([An overview of Russia’s cyberattack activity in Ukraine \(microsoft.com\)](#))

Late March 2022 – (Date approx.) According to a Carnegie Endowment report from December 2022, “within the first several weeks of the war, Russian cyber fires plummeted in number, impact, and novelty. Cyber fires, although still very high relative to prewar baselines, have barely registered on the grand scale of Moscow’s military ambitions and high-intensity combat operations in Ukraine.” ([Russia’s Wartime Cyber Operations in Ukraine: Military Impacts, Influences, and Implications - Carnegie Endowment for International Peace](#))

Late March 2022 – Lawyers and investigators from the UC Berkeley School of Law’s Human Rights Center file a formal Article 15 communication asking the International Criminal Court in the Hague to consider war crimes charges against the GRU-connected Sandworm hacking group for their attacks on Ukraine’s electric grid in late 2015 and 2016. Lindsay Freeman from Berkeley tells *Wired* the HRC wants the court to treat the cyber domain “as an actual domain of warfare, because in this case, it truly is.” It would be the first cyber war crimes case the ICC adjudicated. Among other arguments is the fact that the target of the Sandworm attacks has been civilians, a chargeable offense under the Rome Statute. ([The Case for War Crimes Charges Against Russia’s Sandworm Hackers | WIRED](#); [Russian Cyberattacks Need an International Criminal Court Response | CEPA](#))

Late March 2022 – Ukrainian troops outside Kyiv discover abandoned parts of a Krasukha-4, a key piece of Russia’s electronic warfare (EW) capability designed to jam airborne and satellite-based fire control radars. A major assessment published later by IEEE Spectrum describes the “puzzling failure of Russian EW in the first few months of Russia’s invasion. After nearly a decade of owning the airwaves during a Moscow-backed insurgency in eastern Ukraine, EW was not decisive when Russia went to war in February. The key questions now are, why was this so, what is next for Russian EW in this oddly anachronistic war, and how might it affect the outcome?” ([The Fall and Rise of Russian Electronic Warfare \(ieee.org\)](#))



March 25, 2022 – Further on the theme of Russia’s seemingly muted cyber campaign in Ukraine, a BBC news item cites Western analysts on the presumed reasons why. “Russia believed the government in Kyiv would be toppled quickly and a new pro-Moscow replacement would be put in place. In this scenario, destroying infrastructure would serve little purpose. Destructive cyber-attacks take time to prepare and Moscow's state hackers may also not have had sufficient notice since, like much of the military, they may not have known an invasion was being planned until the last minute. Another reason is that when it comes to a full military conflict, hard military power can be more reliable in destroying targets such as TV towers than cyber-attacks, which are not always guaranteed to work.” Still, Western officials claim there has been no shortage of effort from Moscow. “We have seen broad targeting of Ukrainian networks and systems,” one official told the network. ([Russia hacked Ukrainian satellite communications, officials believe - BBC News](#))

March 26, 2022 – Russian hackers have been targeting Starlink satellite terminals but Elon Musk claims they have all been rebuffed. ([Російські хакери намагаються атакувати супутникові термінали Starlink в Україні - 24 Канал \(24tv.ua\)](#))

March 27, 2022 – The IT Army’s Telegram channel marks a peak of roughly 300,000 subscribers, as noted by cyber expert Stefan Soesanto on Twitter in early December 2022. ([\(9\) Stefan Soesanto on Twitter](#))

March 28, 2022 – The Security Service of Ukraine (SBU) reports that since February 24 it has “eliminated 5 enemy bot farms” with a minimum capacity of 100,000 accounts believed to be spreading false information in the areas of Kharkiv, Cherkasy, Ternopil and the Transcarpathian region. ([Since the beginning of the war, the SBU has eliminated 5 enemy bot farms with a capacity of more than 100 thousand tons. fake accounts \(ssu.gov.ua\)](#))

March 28, 2022 – Ukrtelecom, reportedly the country’s largest fixed line telecommunications company, is hit by a cyberattack reducing its services to 13% of pre-war levels. *Forbes* reports: “While the cyber war side of the Russian invasion of Ukraine has been more muted than most expected, it has been ongoing. Telecom companies have been subjected to heavy cyberattacks but have for the most part avoided any serious deleterious effects.” *Forbes* calls it a “powerful” attack and “the most severe cyberattack since the start of the Russian invasion.” But a later report concludes it was not that serious and that Ukrtelecom was able to recover quickly. ([‘Most Severe’ Cyberattack Since Russian Invasion Crashes Ukraine Internet Provider \(forbes.com\); Why Cyber Dogs Have Yet to Bark Loudly in Russia’s Invasion of Ukraine - Texas National Security Review \(tnsr.org\)](#))

March 28, 2022 – A slightly modified version of the “GoMet” open-source backdoor malware is observed in Ukraine for the first time. Cisco reports later: “Working jointly with Ukrainian organizations, Cisco Talos has discovered a fairly uncommon piece of malware targeting Ukraine — this time aimed at a large software development company whose software is used in various state organizations within

Ukraine. We believe that this campaign is likely sourced by Russian state-sponsored actors or those acting in their interests. As this firm is involved in software development, we cannot ignore the possibility that the perpetrating threat actor's intent was to gain access to source a supply chain-style attack, though at this time we do not have any evidence that they were successful.” ([Cisco Talos Intelligence Group - Comprehensive Threat Intelligence: Attackers target Ukraine using GoMet backdoor](#))

March 28, 2022 – The Defense Department submits its FY2023 budget. In accompanying comments, Secretary Lloyd Austin notes: “U.S. prosperity and military success depend on the cyber resiliency of the Joint Force to execute missions successfully in a contested environment. The FY 2023 Budget allows for continued investment in cyberspace initiatives.” Those investments, totaling \$11.2 billion, include:

- Operationalizing Zero Trust Architecture across Military Departments and Defense Agencies
- Increasing cybersecurity support to the Defense Industrial Base
- Growing the Cyber Mission Force Teams

([The Department of Defense Releases the President's Fiscal Year 2023 Defense Budget > U.S. Department of Defense > Release](#))

March 29, 2022 – The State Service of Special Communications and Information Protection (SSSCIP) of Ukraine posts a bulletin that begins: “Cyberwar is under way and cyberoffenders keep on attempting to cause harm to Ukraine’s information infrastructure or to collect important information. State computer emergency response team (CERT-UA) within the State Service of Special Communication and Information Protection of Ukraine detected spreading malicious emails with the topic “Заборогованість по зарплаті” among the Ukrainian state bodies. Attached to the letter is the document “Заборогованість по зарплаті.xls” that includes legitimate statistical data and macros. At the same time, the attached document also includes encoded data. After the activation, macros decodes this data, creates EXE-file “Base-Update.exe” and launches it on the computer.” ([State Service of Special Communications and Information Protection of Ukraine \(cip.gov.ua\)](#))

March 29, 2022 – In a public service blog post, the U.K. indicates that, of this date, “there are ongoing cyber attacks against Ukrainian infrastructure (including those that we've attributed with our partners to the Russian intelligence services), but we've not seen - and don't expect to see - the massive, global cyber attacks that some had predicted.” ([Use of Russian technology products and services following... - NCSC.GOV.UK](#))

March 29, 2022 – According to a media report today on the state of Ukraine’s Internet, local citizens are creatively adapting to circumstances: “A government app initially developed to help Ukrainians access public services and organize coronavirus tests has been repurposed to allow people to report the position of Russian tanks and soldiers so Ukrainian forces can find and destroy them. Messaging apps have been

used by regular people to coordinate the defense of their hometowns.” ([How are Ukrainians still online one month into the war? - The Washington Post](#))

March 29, 2022 – Axios reports that many Taiwanese are watching the war in Ukraine closely for how a smaller country can respond to a military assault from a larger neighbor. ([Taiwan sees lessons in Ukraine \(axios.com\)](#))

March 30, 2022 – A Presidential Decree requires the suspension of all foreign software purchases for Russian critical infrastructure facilities as of March 31 and prohibits the use of foreign software starting from January 1, 2025. A Ukrainian cyber official writes that a “ban on importing technologies [including radio, electronic, and telecommunication devices] will be a sham, as it will only make the existing practice of purchasing Chinese products and replacing ‘made in China’ labels with ‘from Russian manufacturers’ even more widespread.” (Decree of the President of the Russian Federation, 3-30-22)

March 30, 2022 – Google’s Threat Analysis Group reports “TAG has observed a continuously growing number of threat actors using the [Ukraine] war as a lure in phishing and malware campaigns. Government-backed actors from China, Iran, North Korea and Russia, as well as various unattributed groups, have used various Ukraine war-related themes in an effort to get targets to open malicious emails or click malicious links.” The report continues:

“Financially motivated and criminal actors are also using current events as a means for targeting users. For example, one actor is impersonating military personnel to extort money for rescuing relatives in Ukraine. TAG has also continued to observe multiple ransomware brokers continuing to operate in a business as usual sense.”

TAG’s update lists three groups they are tracking: Curious Gorge, attributed to China’s PLA SSF, which is targeting Ukrainian, Russian, Kazakh, and Mongolian military organizations; COLDRIVER (a.k.a. Calisto) based in Russia which has recently started focusing on East European and NATO entities; and the Belarusian group Ghostwriter. (Later updates identify other malicious groups, including Turla.) ([Tracking cyber activity in Eastern Europe \(blog.google\)](#))

End March 2022 – After Russia implements a significant crackdown on access to Internet providers outside the country, foreign companies are forced into a never-ending “cat-and-mouse game” to keep updating their software in order to prevent Russia from blocking their services. One such company is the Geneva-based Proton, which provides an encrypted email service and VPN access to the web that disguises the identify and location of users. The *New York Times* later profiles Proton as an exemplar of this intensive and risk-laden contest with Moscow. The number of downloads of VPNs in Russia reportedly increases 2,692 percent in March over February, according to the review site Top10VPN.com. ([Inside the Face-Off Between Russia and a Small Internet Access Firm - The New York Times \(nytimes.com\)](#))

End March-Early April 2022 – Ukraine confronts several “huge incidents” in cyberspace during this period, according to a later interview with cybersecurity official Viktor Zhora. In particular, he notes the discovery of “Industroyer2” which can control power flows in electrical utilities. ([Ukraine cyber chief pays surprise visit to 'Black Hat' hacker meeting in Las Vegas | Reuters](#))

March 31, 2022 – President Putin signs a decree aimed at ensuring Russia’s technological independence and the security of its critical information infrastructure. This includes a ban on foreign software for critical information infrastructure facilities without high-level consent. As of January 1, 2025, state authorities will also no longer be allowed to use foreign software at such facilities. ([Putin instructs Cabinet to take steps to make Russia independent from foreign software - Russian Politics & Diplomacy - TASS](#))

March 31, 2022 – German turbine manufacturer Nordex SE discovers a security problem requiring it to shut down its information-technology systems. Ransomware group Conti claims responsibility the following month. ([European Wind-Energy Sector Hit in Wave of Hacks \(wsj.com\)](#))

March 31-April 8, 2022 – Microsoft reports: “This period saw an escalation of attacks on energy infrastructure and targeted efforts to influence Ukrainians’ support for their government ... IRIDIUM took the next steps to launch a destructive attack against the network of a regional energy provider ... Meanwhile, DEV-0586 launched a cyber-enabled influence operation to try to turn Ukrainian citizens against their government ... This was the first instance we had observed such intense anti-government messaging in email.” ([An overview of Russia’s cyberattack activity in Ukraine \(microsoft.com\)](#))

Spring 2022 – Evgenii Serebriakov, a GRU agent who was indicted in the Netherlands in 2018 for cyberespionage, becomes the new commander of the hacking unit Sandworm (Unit 74455), according to Western intelligence sources later cited by *Wired*. Serebriakov previously served as deputy commander of APT28, a.k.a. Fancy Bear, the magazine notes. ([This Is the New Leader of Russia's Infamous Sandworm Hacking Unit | WIRED](#))

April – December 2022 – Russian military and intelligence-linked hackers target and infiltrate the networks of European military, energy and transport organizations. With a lead from Ukrainian officials, Microsoft later discovers that the hackers were exploiting a flaw in Microsoft’s email software, stealing logins and other sensitive information. Microsoft publicly discloses the vulnerability to customers on March 15, 2023. ([Microsoft fixes Outlook zero-day used by Russian hackers since April 2022](#) – BleepingComputer)

April – June 2022 – During the second quarter of 2022, Ukraine experiences an upsurge in cyberattacks and a “significant increase” in the distribution of malware, according to the government’s Vulnerability Detection and Cyber Incidents/Cyber Attacks



System. The period sees a jump in registered and processed cyber incidents from 40 to 64 and a 38% spike in malware distribution. The “absolute majority” of registered incidents are tied to Russian government-funded hacker groups. “The main goal of hackers remains cyber-espionage, disruption of the availability of state information services and even destruction of information systems with the help of wipers,” Ukraine’s cyberagency reports. “By attribution, the absolute majority of registered cyber incidents is related to hacker groups funded by the Russian federation government. In particular, these are UAC-0082/UAC-0113 (related to Sandworm), UAC-0010 (Gamaredon) and others, mentioned in the report.” The main targets of Russian hackers were the mass media, government, and local authorities.

*Infosecurity* magazine quotes Ian Thornton-Trump, CISO at Cyjax, as saying the report shows that secure architecture and best practices are “at least as important, or perhaps even more important, than security technology ... There are great blue team lessons to be learned here.” ([Ukraine's Cyber Agency Reports Q2 Cyber-Attack Surge - Infosecurity Magazine \(infosecurity-magazine.com\); 19b0a96e-8c31-44bf-863e-cd3e0b651f21.pdf \(scpc.gov.ua\)](https://www.infosecurity-magazine.com/19b0a96e-8c31-44bf-863e-cd3e0b651f21.pdf))

April 2022 – The U.S. Army initiates a program to help Ukrainians identify and respond to Russian drones much more efficiently, according to a later report. ([The Ukraine War Is Teaching the US How to Move Intelligence Faster - Defense One](#))

April 2022 – Meta takes down a Russian “troll farm” using Instagram, Facebook, Twitter, YouTube, LinkedIn, and other platforms to sow pro-Russian disinformation. The operation included people previously tied to the infamous Internet Research Agency (IRA). Its modus operandi was to hire people off the street to make up comments, including attributing them to celebrities like Angelina Jolie or Morgan Freeman, according to Meta, which called the campaign “poorly” run and in no way a “dedicated band of patriotic trolls.” Meta found out about it after a journalist working for the Russian outlet Fontanka infiltrated the operation and wrote about it. ([Russian disinformation operation paid for pro-Ukraine war posts: Meta \(rfi.fr\)](#))

April 2022 – The EU announces it plans to restrict Russian payments to European crypto wallets to 10,000 euros in an attempt to prevent the bypassing of restrictions on large bank transfers. ([EU Set to Ban Russian Crypto Payments After 'Sham' Referenda \(coindesk.com\)](#))

April 2022 – Two marketing agencies with ties to Ukraine, 72andSunny and Nebo, form an entity called Torrents of Truth to “spread the truth about the war in Ukraine among Russians.” They take advantage of Russian pirating of Western films (after Western streaming services suspend operations in Russia) by uploading videos describing what Russia is doing in Ukraine that are embedded in well-known movies or shows. The videos pop up in the course of viewing like an advertisement. ([How Ukrainians are using pirated movies to bring war's reality to Russian viewers - The Record by Recorded Future](#))

April 2022 – In an example of creative volunteer hacktivism, a Ukrainian hacker named Oleksandr launches a DDoS attack against a Russian service called “Chestny Znak” which verifies the authenticity of all Russian goods by scanning them for a unique number and barcode required by Russian law. The attack takes the service offline for about four days. “The economic losses were pretty high, I think. It was mind-blowing,” Oleksandr tells the BBC later. ([Meet the hacker armies on Ukraine's cyber front line - BBC News](#))

April 2022 – In development since February 2022, Black Basta ransomware group first becomes operational, and soon highly active, in April 2022. According to SecurityWeek, the Russian-linked group uses “malware to encrypt files on compromised systems ... they steal large amounts of information from victims in an effort to increase their chances of getting paid,” employing a “double extortion” strategy. Due to the sophisticated nature of the attacks in the group’s early stages, researchers suggested the group may be linked to other Russian-based hacking groups, but it is not until November 2022 that SentinelLabs specifically ties Black Basta ransomware to Russian cybercrime group FIN7. ([Black Basta Ransomware Becomes Major Threat in Two Months](#) – SecurityWeek; [Black Basta Ransomware | Attacks Deploy Custom EDR Evasion Tools Tied to FIN7 Threat Actor](#) – SentinelLabs)

April 1, 2022 – According to a later report by Trustwave, “the IT Army launch[es] an automated chatbot on Telegram that responds to questions and provides an instruction guide detailing how to execute DDoS attacks.” Shortly afterwards, the group creates a website providing specifics on how to launch a DDoS attack. ([Development of the Ukrainian Cyber Counter-Offensive | Trustwave](#))

April 5, 2022 – USCYBERCOM Commander Paul Nakasone testifies to the Senate and House armed services committees. His prepared statement includes the following:

“Russia’s invasion of Ukraine demonstrated Moscow’s determination to violate Ukraine’s sovereignty and territorial integrity, forcibly impose its will on its neighbors and challenge the North Atlantic Treaty Organization (NATO). Russia’s military and intelligence forces are employing a range of cyber capabilities, to include espionage, influence and attack units, to support its invasion and to defend Russian actions with a worldwide propaganda campaign.

“U.S. Cyber Command (with NSA) has been integral to the nation’s response to this crisis since Russian forces began deploying on Ukraine’s borders last fall. We have provided intelligence on the building threat, helped to warn U.S. government and industry to tighten security within critical infrastructure sectors, enhanced resilience on the DODIN (especially in Europe), accelerated efforts against criminal cyber enterprises and, together with interagency members, Allies, and partners, planned for a range of contingencies. Coordinating with the Ukrainians in an effort to help them harden their networks, we deployed a hunt [forward] team who sat side-by-side with our partners to gain critical insights that have increased homeland defense for both the United States and Ukraine. In addition, USCYBERCOM is proactively ensuring the security and availability of strategic command and control

and other systems across the Department. We have also crafted options for national decision makers and are conducting operations as directed.

“When Moscow ordered the invasion in late February, we stepped up an already high operational tempo. We have been conducting additional hunt forward operations to identify network vulnerabilities. These operations have bolstered the resilience of Ukraine and our NATO Allies and partners. We provided remote analytic support to Ukraine and conducted network defense activities aligned to critical networks from outside Ukraine – directly in support of mission partners. In conjunction with interagency, private sector and Allied partners, we are collaborating to mitigate threats to domestic and overseas systems.

“These measures were made possible by the patient investments in cyberspace operations capabilities and capacity over the last decade, as well as by the lessons that we as a Department and a nation have learned from operational experience.”

(<https://www.cybercom.mil/DesktopModules/ArticleCS/Print.aspx?PortalId=56&ModuleId=4502&Article=2989087>)

April 5, 2022 – As part of an operation months in the making (well before Russia’s invasion of Ukraine), German police take down Hydra, a dominant presence in illegal Russian online activity including narcotics sales, forged documents, and money laundering. “After the downfall of Hydra, much of its customer base and merchants regrouped on RuTor,” according to a report in Al Jazeera in late 2022. RuTor is described as “an online forum that is one of the Russian internet’s oldest cybercrime hangouts.” The site was subsequently the object of rumors that it was under the control of the SBU, which in turn made it a target of DDoS attacks from the pro-Russia group Killnet. Experts later see the strikes not as being against narcotics marketplaces but against sites with ties to Ukraine, reflecting a “definite change” in the focus of DDoS instigators. ([Russia-Ukraine war reaches dark side of the internet | Russia-Ukraine war News | Al Jazeera; TextDocumentTemplate \(website-files.com\)](#))

April 5, 2022 – During his testimony to the armed services committees, Nakasone says that the Ukraine experience is teaching USCYBERCOM a great deal. “My sense is we are learning a tremendous amount of our operations right now in support of crisis in the Ukraine ... We’re a different force today than we were even four years ago when I took over.” ([Cyber Mission Force Set to Add More Teams > U.S. Department of Defense > Defense Department News](#))

April 8, 2022 – A Ukrainian electrical substation is hit by the GRU-linked Sandworm hacker group, also known as Unit 74455. The malware used is a variant of Industroyer or Crash Override, called Industroyer2. *Wired* writes: “It signals that Russia’s most aggressive cyberattack team [has] attempted a third blackout in Ukraine, years after its historic cyberattacks on the Ukrainian power grid in 2015 and 2016, still the only confirmed blackouts known to have been caused by hackers.” The attack includes various kinds of wiper software. Ukrainian authorities say “the intended disruption was huge” but claim it was “promptly detected and mitigated.” ([Russia's Sandworm Hackers Attempted a Third Blackout in Ukraine | WIRED](#))

ESET's principal threat researcher says later, "Our analysis found that threat was bigger than expected. It was a new version of Industroyer, something which we hadn't seen in the last five years." Another ESET researcher tells a Black Hat 2022 audience that Industroyer2 contained hardcoded configurations, indicating prior planning, and was specifically aimed at crippling circuit-breaker failure protections for systems used by the victimized company. ESET said the programmers made mistakes that helped mitigate the incident. "The threat shouldn't be hyped but also should not be downplayed or underestimated," the researcher added. "These threats are serious, but they can be thwarted by proper security measures." ([Industroyer2: How Ukraine avoided another blackout attack \(techtarget.com\)](#))

For an earlier account of evidently the same incident, see the following link. Among other things, it reports that Ukrainian experts consulted with Microsoft in the wake of the event, but Microsoft declined to comment initially. ([Ukraine Thwarts Cyberattack on Electric Grid, Officials Say \(wsj.com\)](#))

Researchers believe that if the attack had not been thwarted, it would have caused blackouts for two million people and could have been the most serious cyberattack against Ukraine since the Russian invasion. (Ukrainian power grid 'lucky' to withstand Russian cyber-attack – BBC)

April 11, 2022 – German firm Deutsche Windtechnik is hit by a ransomware attack. The next morning (April 12) workers discover that the company's internal IT systems have been targeted. By the following day, most problems are resolved and the company does not contact the hackers. ([European Wind-Energy Sector Hit in Wave of Hacks \(wsj.com\)](#))

April 11, 2022 – "Ukrainians may not be able to use GPS because there are jammers around that prevent them from receiving and using the signal effectively," according to Gen. David Thompson, vice chief of space operations at Space Force. Space Force is charged with monitoring U.S.-operated GPS satellites. (A Space Force officer quoted by NBC Nightly News avers that Russia and China very likely avail themselves of the access provided to all users via these satellites.) NBC reports that Russia has also apparently jammed GPS systems used by civilian aircraft along the Russian-Finnish border. Moscow has not attacked any U.S. satellites but it did test fire a weapon that destroyed one of its own satellites, NBC reports. According to Gen. Thompson, this was "a very clear statement about their intention to threaten our capabilities." ([Watch NBC Nightly News with Lester Holt Excerpt: Russia is jamming U.S.-provided GPS signals in Ukraine, U.S. general says - NBC.com](#))

April 12, 2022 – Cloudflare reports a rise in DDoS attacks in the first quarter of the year. In the Russia and Ukraine space it finds that online and broadcast media have been hardest hit:

- "Russian Online Media companies were the most targeted industries within Russia in Q1. The next most targeted was the Internet industry, then Cryptocurrency, and then Retail. While many attacks that targeted Russian



Cryptocurrency companies originated in Ukraine or the US, another major source of attacks was from within Russia itself.

- “The majority of HTTP DDoS attacks that targeted Russian companies originated from Germany, the US, Singapore, Finland, India, the Netherlands, and Ukraine. It’s important to note that being able to identify where cyber attack traffic originates is not the same as being able to attribute where the attacker is located.
- “Attacks on Ukraine targeted Broadcast Media and Publishing websites and seem to have been more distributed, originating from more countries — which may indicate the use of global botnets. Still, most of the attack traffic originated from the US, Russia, Germany, China, the UK, and Thailand.” ([DDoS Attack Trends for 2022 Q1 \(cloudflare.com\)](#))

April 13, 2022 – The Russian-language news outlet Meduza, based in Latvia, publishes an analysis of tens of thousands of leaked records from Russia’s Roskomnadzor (see Early March entry), described here as “Russia’s federal censor.” The article notes that Roskomnadzor starting keeping daily track of protest sentiment in 2020. ([The hunt for ‘antimilitarism’ Leaked documents indicate that Russia’s federal censor has been monitoring the Internet for peace activism since at least 2020 — Meduza](#))

April 14, 2022 – CERT-UA reports a cyberattack on Ukrainian government organizations exploiting a vulnerability in the Zimbra Collaboration Suite. ([CERT-UA](#))

April 14, 2022 – The Russian guided missile cruiser *Moskva*, flagship of the Black Sea Fleet, sinks in the Black Sea after being hit by two Ukrainian Neptune missiles, according to both Ukrainian and U.S. Defense Department officials. Recorded Future later notes that Ukraine’s battlefield management system Delta played a part in the strike. ([Joker DPR and the Information War \(recordedfuture.com\)](#))

Mid-April 2022– According to reports, by this time Ukrainian cyber specialists have identified at least 14 separate hacker groups with ties to Russian and Belarusian special services. In addition, special agencies (possibly units of Russian special services) from the Donetsk and Luhansk people’s republics are believed to be involved. (Dmytro Dubov, “Russia’s in Ukraine: The War in Cyberspace” (Series No. 2)

Mid-April 2022 – According to IBM Security X-Force, “In mid-April, ITG23 used phishing emails to deliver a malicious Excel file (described in detail below) to targets in Ukraine that downloaded and installed IcedID. ITG23 has a very close relationship with the IcedID group dating back several years and is likely relying on IcedID to obtain initial access into a victim’s environment ... According to CERT-UA, the campaign targeting consisted of “mass distribution among citizens” of Ukraine, suggesting less discriminate targeting within the country.” ([Unprecedented Shift: The Trickbot Group is Systematically Attacking Ukraine \(securityintelligence.com\)](#))

Mid-April 2022 – [See previous entry] According to IBM Security X-Force, “Shortly after the ... campaign in mid-April, ITG23 [Conti group] used a similar malicious Excel file to download a CobaltStrike sample which used the ITG23 “Tron” crypter. CERT-UA called this campaign a ‘cyberattack on state organizations of Ukraine’ ... A malicious Excel spreadsheet used in this campaign was uploaded to the VirusTotal repository from Ukraine with the filename “Військові на Азовсталі” (“The military in Azovstal”). The reported targeting of state organizations and direct download of CobaltStrike suggest this was a more targeted attack against specific victims.” ([Unprecedented Shift: The Trickbot Group is Systematically Attacking Ukraine \(securityintelligence.com\)](https://www.securityintelligence.com))

Mid-April – December 2022 – The hacking group STRONTIUM (a.k.a. APT28, Sednit, Sofacy, and Fancy Bear) steals credentials from a number of government and other organizations by means of malicious Outlook notes and tasks, which it then uses to gain access to Outlook emails, according to a private Microsoft threat report not disseminated until mid-March 2023. BleepingComputer reports at that time that Microsoft assesses that the breach affected fewer than 15 government, military, energy, and transportation organizations. ([Microsoft fixes Outlook zero-day used by Russian hackers since April 2022 \(bleepingcomputer.com\)](https://www.bleepingcomputer.com))

April 18, 2022 – Costa Rica’s Finance Ministry is the first to report problems with a number of its computer systems in what turns out to be a large-scale ransomware attack by the Russian-based Conti group. ([Cyberattack Causes Chaos in Costa Rica Government Systems | SecurityWeek.Com](https://www.securityweek.com))

April 20, 2022 – CISA releases a joint Cybersecurity Advisory (CSA) along with other Five Eyes members Australia, Canada, New Zealand, and the United Kingdom. “The intent of this joint CSA is to warn organizations that Russia’s invasion of Ukraine could expose organizations both within and beyond the region to increased malicious cyber activity .... Evolving intelligence indicates that the Russian government is exploring options for potential cyberattacks.” The advisory continues: “Additionally, some cybercrime groups have recently publicly pledged support for the Russian government.” ([Russian State-Sponsored and Criminal Cyber Threats to Critical Infrastructure | CISA](https://www.cisa.gov))

April 20, 2022 – The Czech News Agency reports: “According to the National Office for Cyber and Information Security, hackers have attacked some Czech websites, including České dráhy (Czech railways), some regional airports, and the civil service server operated by the Interior Ministry. Russian hackers attacked the Internet systems of the Czech state and private institutions, but no information and no private data of citizens have been leaked, Interior Minister Vít Rakušan said at a press conference after a cabinet meeting today.” ([Russian hackers target Czech websites in a series of cyberattacks - Prague, Czech Republic \(expats.cz\)](https://expats.cz))

April 22, 2022 – CERT-UA releases a list of the top five groups that have hit Ukraine in the first quarter of 2022. The agency has recorded 802 cyberattacks during the period compared to 362 a year ago:

1. UAC-0010 aka Armageddon (GammaLoad, GammaDrop, HarvesterX): APT (advanced persistent threat), a group backed by the Russian FSB.
2. UAC-0041 (AgentTesla, XLoader): Russian hackers.
3. UAC-0056 (Pandora hVNC, RemoteUtilities, GrimPlant, GraphSteel): Russian hackers and cyber spies.
4. UAC-0051 aka UNC1151: APT, a group allegedly linked to special services of the Republic of Belarus.
5. UAC-0028 aka APT28: APT, a group allegedly linked to GRU (Main Intelligence Directorate) of the Russian Federation.

The agency release adds: “UAC-0041 and UAC-0056, associated by the international community with Russian hackers, are the ones being unusually active. They exploit the current military issues. Most likely, the Russian intelligence service shares data with these groups.” ([Five hacker groups that attack Ukraine the most \(cip.gov.ua\)](#))

April 2022 – Since April 2021, U.S. employers have initiated 714,548 job postings for cybersecurity-related jobs, a 43% spike over the previous year, according to findings by [CyberSeek](#), a joint endeavor that includes the Commerce Department’s National Initiative for Cybersecurity Education (NICE). Almost 40% of those postings appeared in the first quarter of 2022. “Demand for cybersecurity jobs increased by 43% in the 12-month period compared to a nearly 18% increase in demand across the entire employment market, according to a press release. “Employers are desperate to find enough skilled workers to counter constantly growing digital threats,” the release notes. ([Cybersecurity Hiring Momentum Ramps Up, New Data from CyberSeek™ Reveals \(comptia.org\)](#))

April 25, 2022 – “The DDoS landscape in Q1 2022 was shaped by the ongoing conflict between Russia and Ukraine,” according to a Kaspersky report issued on this date. Quarterly figures jumped 450% from the same period last year. “The reason for this growth is obvious: the crisis in Ukraine led to a cyberwar, which could hardly fail to impact the statistics. Looking at the distribution of DDoS attacks by week, we see that the peak of new attacks occurred in the eighth week of 2022, that is, February 21–27, and we repelled the largest number of DDoS attacks that week on February 25.” ([Kaspersky DDoS report, Q1 2022 | Securelist](#))

April 26, 2022 – (Date approx.) Russian media outlet RT announces the launch of a Telegram channel (@video\_language) effort to use videos to help spread Russian versions of events relating to the Ukraine war on social media. The videos are subtitled in 18 languages. A later study by the firm Nisos concludes that the initiative is a wide-ranging attempt to evade EU and social media platform bans on RT and Sputnik. The method involves uploading videos to Telegram, often with RT watermarks removed, then downloading the material to Twitter and other platforms in a way that eliminates any indicators of a connection to Russian state

media. Nisos located hundreds of social media accounts that were involved and tied them to the Russian military, diplomatic missions, or state media. Nisos characterized as “coordinated inauthentic behavior” (CIB).

([Nisos RTs Information Militia 20220913 \(hubspotusercontent-na1.net\)](#); [Experts: Russia finding new ways to spread propaganda videos | AP News](#))

Late April 2022 – According to IBM Security X-Force, “In late April, CERT-UA released details of a phishing campaign delivering Meterpreter which they assessed was associated with the Trickbot group. The campaign used emails ... to deliver an ISO image file. CERT-UA stated that the attack was against ‘the state authorities of Ukraine.’ Similar to [a previous] campaign ... the reported targeting of state organizations and direct download of Meterpreter suggest this campaign was directed at specific targets.” ([Unprecedented Shift: The Trickbot Group is Systematically Attacking Ukraine \(securityintelligence.com\)](#))

Late April 2022 – Dmytro Budorin, CEO of a Ukrainian cybersecurity startup named Hacken, tells *Wired* that his company has set up a “bug bounty program” to encourage reporting on Russian computer security flaws. He claims to have received 3,000 reports including “details of leaked databases, login information, and more severe instances where code can be run remotely on Russian systems,” the article states. The information is then validated and reported to government authorities, Budorin tells the magazine: “You don’t go through the main door ... You go through the regional offices. There are so many bugs, so many open windows.” ([Russia Is Being Hacked at an Unprecedented Scale | WIRED](#))

April 27, 2022 – Microsoft’s Digital Security Unit releases a report detailing its observations to date of Russia’s “hybrid war against Ukraine.” Since just prior to the February invasion, the report indicates at least six nation-state actors aligned with Russia have launched over 237 operations against Ukraine, along with “broad espionage and intelligence activities.” “It is unclear whether computer network operators and physical forces are just independently pursuing a common set of priorities or actively coordinating. However, collectively, the cyber and kinetic actions work to disrupt or degrade Ukrainian government and military functions and undermine the public’s trust in those same institutions.” ([An overview of Russia’s cyberattack activity in Ukraine \(microsoft.com\)](#))

April 27 – May 11, 2022 – During this period, numerous Russian state-sponsored groups have undertaken cyber-espionage attacks, according to Accenture, which compiled the following list:

- “A recent Gamaredon (a.k.a. WINTERFLOUNDER) operation leveraged Ukrainian-language and English-language lure documents purportedly related to humanitarian assistance for Ukrainian refugees. Targets reportedly included Latvia, a NATO member.
- “ACTI identified an overlap in infrastructure between Gamaredon and the cyber criminal Cobalt Group’s malware, suggesting the groups possibly share tools.



- “The SolarWinds cyber espionage actors have undertaken new phishing campaigns against European, US, and Asian diplomats; as part of these operations, they introduced two malware families in 2022 and sought to evade detection through retooling and abuse of Atlassian's Trello service, according to Mandiant.
- “A newly identified group that Mandiant calls UNC3524 has TTPs that overlap with APT28 (a.k.a. SNAKEMACKEREL) and APT29 (a.k.a. JACKMACKEREL). Masquerading as the Computer Emergency Response Team for Ukraine (CERT-UA), SNAKEMACKEREL sent malicious messages asking recipients to download an “UkrScanner” that drops the CredoMap\_v2 malware. The threat actors use a subdomain of pipedream[.]net, possibly in a deliberate taunt of using the name of the PIPEDREAM industrial control systems (ICS) malware.” ([Global incident report: Russia Ukraine Crisis, May 13 | Accenture](#))

April 13, 2022 – CISA, the Department of Energy, the FBI, and the NSA issue a joint Cybersecurity Advisory (CSA) (revised May 25, 2022) about an alarming new threat from APT actors who “have exhibited the capability to gain full system access to multiple industrial control system (ICS)/supervisory control and data acquisition (SCADA) devices.” The newly discovered malware is dubbed PIPEDREAM by the industrial security firm Dragos and is believed to be of Russian origin, according to Mandiant.

Almost a year later, Dragos CEO Robert M. Lee expands on the subject to a reporter. Within the first weeks of Russia’s invasion, he says, hackers belonging to a group Dragos calls Chernovite get “very close” to taking a dozen U.S. electric and gas facilities offline. “This is the closest we’ve ever been to having U.S. or European infrastructure, I’d say U.S. infrastructure, go offline,” Lee says. “It wasn’t employed on one of its targets, they weren’t ready to pull the trigger, they were getting very close.”

He gives no specifics as to how the attack was averted but says that the effort involved private sector groups collaborating with several government agencies, including CISA, the Department of Energy, the FBI, and NSA (see link below to the April 13 CSA). Lee adds that the malware’s ability to work across different industrial control systems, not just a single system, is what makes it especially dangerous. ([APT Cyber Tools Targeting ICS/SCADA Devices | CISA](#); [Suspected Russian malware's likely target was LNG facilities - The Washington Post](#); [Russian-linked malware was close to putting U.S. electric, gas facilities ‘offline’ last year - POLITICO](#); [CHERNOVITE's PIPEDREAM Targeting Industrial Control Systems \(ICS\) \(dragos.com\)](#))

April 27, 2022 – The group Legion claims to carry out cyber operations in support of Killnet. ([Dark Covenant 2.0: Cybercrime, the Russian State, and the War in Ukraine \(recordedfuture.com\)](#))

April 28, 2022 – President Biden submits a huge \$33 billion aid request to Congress for Ukraine. A fact sheet released to the public indicates the package includes

“accelerated cyber capabilities.” ([White House Calls on Congress to Provide Additional Support for Ukraine | The White House](#))

April 28, 2022 – The United States and some 55 other countries pledge their commitment to a free and open Internet amid rising concerns about an emerging “splinternet” stemming from Russia’s numerous steps to block access to the worldwide web to its citizens along with many other elements of its information war in and around Ukraine. (White House statement, 4-28-2022)

April 28, 2022 – CISA and FBI update an earlier advisory “to include additional Indicators of Compromise (IOCs) for WhisperGate and technical details for HermeticWiper, IsaacWiper, HermeticWizard, and CaddyWiper destructive malware, all of which have been deployed against Ukraine since January 2022.” ([AA22-057A Destructive Malware Targeting Organizations in Ukraine.pdf \(cisa.gov\)](#))

April 28, 2022 – Cybersecurity firm Fortinet posts an article seeking to provide historical and technical context for the recent spike in wiper malware activity since Russia’s invasion of Ukraine. ([An Overview of the Increasing Wiper Malware Threat | FortiGuard Labs \(fortinet.com\)](#))

April 29, 2022 – Romania’s National Directorate for Cyber Security reports: “Today, a series of Distributed Denial of Service (DDoS) attacks took place on sites belonging to public institutions and private organizations in Romania .... The attack was claimed by the cybercrime group ‘Killnet’ on a communication channel on Telegram and is justified by them by the fact that the Romanian state supports Ukraine in the military conflict with Russia.” ([Press release: .ro sites affected by a DDoS attack \(distributed denial of service\) \(dnsc.ro\)](#))

April 29, 2022 – At a Pentagon background briefing a reporter asks for specifics about “accelerated cyber capabilities” for Ukraine following yesterday’s announcement at the White House. “Senior Defense Official: We’re just talking about being able to – to continue to help Ukraine improve their cyber resilience, and some of those funds will be ... additional to ongoing efforts to improve the Ukrainians’ cyber – cyber defense and resilience capabilities, and I don’t think we want to get into more than that.” ([Senior Defense Official Holds a Background Briefing > U.S. Department of Defense > Transcript](#))

End April 2022 – Ukraine’s IT Army launches its own website. ([Russia Is Being Hacked at an Unprecedented Scale | WIRED](#))

April 30, 2022 – Mobile communications and Internet shut down across the Kherson region, Radio Free Europe reports. “The fact that this is not an accident was announced by one of the leading specialists of the Vodafone mobile operator in Kherson. Kyivstar operated in some districts of the region, but without the Internet, Suspilne reported.” The next day, SSSCIP reports that fiber-optic main lines were broken and equipment disconnected from their power supply. By May 3, mobile

communications begin to reappear and Internet is 85% restored. (["They are afraid of resistance." Why does Russia seize mobile communications and the Internet in the Kherson region? \(radiosvoboda.org\)](#))

*Wired* later reports: "KhersonTelecom first switched its internet traffic to a Russian network on April 30, before flipping back to Ukrainian connections for the majority of May. However, things appear to have shifted permanently since May 30. All of KhersonTelecom's traffic is now being routed through Miranda Media, a Crimea-based company that's itself connected to Russian national telecom provider Rostelecom. (Miranda Media was set up after Putin annexed Crimea in 2014). The day after KhersonTelecom made its latest switch, state-controlled Russian media outlet RIA Novosti claimed the Kherson and Zaporizhzhia areas were officially being moved to Russian internet connections—days earlier, the outlet said the regions were also going to start using the Russian telephone code +7." ([Russia Is Taking Over Ukraine's Internet | WIRED](#))

May 2022 – After a request from the Moldovan government earlier in the Spring, the EU approves 8 million euros (about \$8.1 million) to help build the country's cybersecurity infrastructure. The U.S. has provided approximately \$11 million in cybersecurity and anti-cybercrime assistance since 2018, according to Kent Doyle Logsdon, the U.S. ambassador to Moldova. Washington is also helping with plans to create the country's first national computer emergency response team (CERT). Iurie Turcanu, Moldova's deputy prime minister for digitalization says the number of cyberattacks has risen over the course of the conflict but none has been significant. The country's biggest challenge is locating and paying qualified experts. ([Moldova Plans Cyber Overhauls Amid War in Neighboring Ukraine - WSJ](#))

May 2022 – Three months into the war, the Ukraine experience appears far from "imminent" and cyber operations are significantly overrated, according to an article published by the Center for Security Studies at ETH Zurich. Lennart Maschmeyer and Myriam Dunn Cavelty argue that cyber ops are "either too slow, too weak, or too volatile to provide significant strategic value in hybrid conflict and war." They add that while such operations have value for intelligence gathering and "mildly disruptive attacks," they suffer from "an operational trilemma" that limits the "speed, intensity, and control that cyber operations can achieve." ([PP10-3 2022-EN.pdf \(ethz.ch\)](#))

Reflecting the ongoing debate over the potential and actual role of cyber in a kinetic conflict, the article prompts a reply posted on Google Docs by Dave Aitel (identified in Wikipedia as a former NSA research scientist, author, software company founder, and "infrequent guest on the Fox News Channel"), which offers a number of counter-arguments. Notably, Maschmeyer attaches several comments to Aitel's critique. ([Goodbye Cyberwar - Google Docs](#); [Dave Aitel - Wikipedia](#))

May 2022 – The IT Army adds an attack automation function to its Telegram chatbot, according to a later report by Trustwave. The move lets volunteers "grant bot access to their cloud resources. This action could allow a coordinated attack from all

available servers.” ([Development of the Ukrainian Cyber Counter-Offensive | Trustwave](#))

May 1, 2022 – The Intelligence and Security Service of Moldova (SIS) reports a cyberattack which it attributes to the pro-Russia Killnet group. “On 01.05.2022, ... at approximately 02:00, a number of web pages belonging to public authorities were subjected to DDoS (Distributed Denial of Service) attacks. The attack follows similar actions reported in Romania within the past few days. ([Killnet attacked several websites of state institutions in the Republic of Moldova – europe-cities.com](#))

Early May 2022 – According to IBM Security X-Force, “In early May, X-Force discovered a campaign using a malicious Excel file very similar to those used in the first two campaigns [see “Mid-April” entries above] that downloaded AnchorMail, a backdoor developed by ITG23 and based on their AnchorDNS malware. It is unusual to see Anchor backdoors downloaded directly as the first stage of an attack; typically, they are installed later in the infection. Their use suggests that this campaign may have been targeted against specific individuals or organizations, although we lack information on the specific target set.” ([Unprecedented Shift: The Trickbot Group is Systematically Attacking Ukraine \(securityintelligence.com\)](#))

Early May 2022 – Recorded Future assesses in mid-year that: “Since at least early May 2022, Russian influence networks, including state-controlled media, known covert intelligence outlets, and known propaganda and disinformation amplifiers, have almost certainly been conducting several multifaceted information operations to undermine and divide the Western coalition on Ukraine and influence public opinion of Russia’s war against Ukraine favorably toward Russia. These information operations almost certainly aim to undermine and divide the Western coalition on Ukraine both directly, by creating or exacerbating divisions between Western coalition countries, and indirectly, by influencing European populations to oppose their governments’ support of Ukraine and negative policies toward Russia.” RF believes the main targets are France, Germany, Poland, and Turkey. “Notably, many of the aforementioned narratives align with an unverified analytical note from the Fifth Service of Russia’s Federal Security Service (FSB), reportedly intercepted and published by the Security Service of Ukraine (SBU) on June 5, 2022” (see entry below). RF says they have “made best efforts to notify all affected organizations of the identified activity to support incident response and remediation investigations. Where direct notification was impossible, we notified relevant third-party organizations with a national cyber security mandate.” ([Message from Recorded Future](#))

Early May 2022 – Drone programmers release software that allows operators to disguise drones from DJI’s AeroScope tracking program, according to a later report. Russian forces are believed to be using AeroScope to track and destroy Ukrainian commercial drones. DJI has previously insisted their program “cannot be turned off” but an anonymous operations officer in Ukraine’s 68<sup>th</sup> Jager brigade tells C4ISRNET that Ukrainian forces learned about the program, called CIAJeepDoors, which can



send a command to switch off the Chinese firm's Remote ID function. Other Ukrainian units reportedly use different software to the same end. ([How Ukraine learned to cloak its drones from Russian surveillance \(c4isrnet.com\)](#))

May 3, 2022 – Slate highlights “Ukraine’s caustic wartime humor” as an unexpected but evidently effective byproduct of the conflict – from postage stamps of a soldier giving the bird to the *Moskva* warship to memes of farmers towing away Russian tanks to a wide variety of YouTube videos. As the war goes on, Internet trolling of Moscow by Ukrainian and like-minded souls escalates, leading to the creation of memorable groups like the North Atlantic Fellas Organization. ([Ukraine’s wartime humor: where it came from. \(slate.com\)](#); [With NAFO, the North Atlantic Fellas Organization, Ukraine turns the trolls on Russia - The Washington Post](#))

May 4, 2022 – Gen. Paul Nakasone touches on the “hunt forward” concept at a Vanderbilt University security summit: “Think how much this has changed [since 2018], even in the past several months ... What have we seen with the Russia-Ukraine crisis? Information that’s used to build and sustain a coalition. Information that’s used to expose malign behavior. Information that’s shared to increase a partner’s knowledge of an adversary.” Army Maj. Gen. Joe Hartman, Cyber National Mission Force commander, adds that operations provide a “key asymmetric advantage that our adversaries don’t have ... We get to find our adversaries in foreign space, before they’re able to come to America and compromise our network. And while we do that, we get to make our partners and allies safer.” ([US cyber squad boosts Lithuanian defenses amid Russian threat \(airforcetimes.com\)](#))

May 4, 2022 – U.S. government and private sector leaders discuss legal and normative issues raised by the Ukrainian government’s global invitation to join its IT Army. “I will tell you that the idea of the civil vigilantes joining in a nation-state attack is unwise, right? I really think it is,” Rob Joyce, NSA’s director of cybersecurity, tells a Vanderbilt University emerging threats conference. For one thing, “it’s illegal. But it’s also unhelpful, because one of the things we talked about is we’re trying to get Russia to take account for the ransomware attacks and hacks that come out of Russia and emanate.” Kevin Mandia, CEO of Mandiant, agrees. “You can’t have the private sector influencing the doctrine between nations .... You don’t have us fighting on air, land and sea without being deputized or part of a force and with an agenda and a mission plan.” ([NSA cyber boss seeks to discourage vigilante hacking against Russia \(c4isrnet.com\)](#))

May 5, 2022 – Detector Media reports that the “Ukrainian Telegram segment has changed significantly since the beginning of the full-scale war.” Specifically, the group has found 88 new Telegram channels opened by Russia, mainly in the South, East, and North – i.e. in occupied territories. “It is important to understand that it is impossible to check whether the Telegram channels’ subscribers are bots or similar to bots because the social network does not provide a list of profiles subscribed to the channel. It is also impossible to verify the geography of subscribers. However, the authenticity of the Telegram channels’ popularity can be judged by other

indicators. In particular, the dynamics of subscribers' growth." ([«Now we will live to the fullest!». How and why Russia has created a Telegram channels network for the occupied territories of Ukraine - Детектор медиа. \(detector.media\)](#))

May 6, 2022 – According to reports cited by Accenture, “On 6 May, the pro-Russia Killnet group vowed revenge after UK officials arrested a member on suspicion of attacking Romanian government sites. The Killnet Telegram site read: ‘If he is not released within 48 hours I will destroy your Romania, Great Britain and Moldova.’ Addressing the UK, Killnet said: ‘I will destroy your entire information structure and even your Ministry of Health. All ventilators will be attacked.’” ([Global incident report: Russia Ukraine Crisis, May 13 | Accenture](#))

May 6, 2022 – The State Department offers a reward of up to \$10 million for information on key leaders of the Conti ransomware group and up to \$5 million for information “leading to the arrest and/or conviction” of anyone conspiring to be part of a “Conti variant ransomware incident.” The FBI indicates that Conti has conducted over 1,000 attacks and received payouts of more than \$150,000,000. Most recently, in April 2022, the group hit the Government of Costa Rica.

“This reward is offered under the Department of State’s Transnational Organized Crime Rewards Program (TOCRP). The Department manages the TOCRP in close coordination with our federal law enforcement partners as part of a whole of government effort to disrupt and dismantle transnational organized crime globally, including cybercrime.” ([Reward Offers for Information to Bring Conti Ransomware Variant Co-Conspirators to Justice - United States Department of State](#))

May 8, 2022 – In anticipation of Russia’s Victory Day celebrations on May 9, Ukraine’s “IT Army” launches an attack on RuTube, a private Russian competitor of YouTube, which the perpetrators say is the “main information center for Russian false propaganda.” On the night of May 8, the group changes administrator passwords, blocks access cards, deletes “dozens of petabytes of information,” and “demolishe[s] all systems.” RuTube restores partial access on May 11 with help from Russian cybersecurity company Positive Technologies. The IT Army takes credit for the attack on May 14. One analyst later calls it the organization’s “first destructive offensive cyber operation” since the start of the war. ([Cyber-Reports-2022-06-IT-Army-of-Ukraine.pdf \(ethz.ch\)](#))

May 9, 2022 – The Biden administration submits an appendix to its FY2023 budget request, which includes the following description State Department foreign operations as part of a \$420 million item request for Ukraine:

“U.S. assistance will support Ukraine as it defends itself against the further invasion by Russia, providing increased economic and security assistance to help ensure continuity of government functions, promote the resilience of the Ukrainian people, and assist Ukraine in defending its territorial integrity. The U.S. assistance program in Ukraine will remain the largest in the region. Funding will support energy and cyber security investments and technical assistance, including those efforts needed to protect critical government services, industries, and

infrastructure; efforts to counter disinformation; initiatives to document and hold perpetrators accountable for human rights abuses and war crimes and build a basis for future peace and reconciliation efforts; and reconstruction efforts ....

Programming will continue to deter the Kremlin's malign activities and disinformation efforts, including by supporting independent media, defending the freedom of expression, and promoting internet freedom and access. U.S. assistance will support Ukraine's Euro-Atlantic trajectory, boost the capacity of media sources and outlets, increase access to diverse and credible information sources, and enhance cybersecurity nationwide...." ([FY-2023-Congressional-Budget-Justification-Appendix-2-final-5-9-2022.pdf \(state.gov\)](#))

May 9, 2022 – Italian authorities say they prevented DDoS attacks from sabotaging the final round and voting stages of the annual Eurovision Song Contest in Turin, after combing Killnet-related Telegram channels in search of the hackers' location and other relevant information. (The Ukrainian band Kalush Orchestra wins the competition, leaping from fourth place, based on judging, to the top spot, thanks to a surge of fan voting.) ([Russian hackers declare war on 10 countries after failed Eurovision DDoS attack | IT PRO](#); [At Eurovision 2022, Ukraine's Kalush Orchestra wins - The Washington Post](#))

May 10, 2022 – Cyber security principals from the 5 Eyes, EU, and other allied states meet at the NCSC's Cyber UK conference in Newport to discuss shared threats. ([Russia behind cyber attack with Europe-wide impact an hour... - NCSC.GOV.UK](#))

May 10, 2022 – CISA updates an earlier alert about threats to satellite communications (SATCOM) networks; the update specifically attributes the threat to "Russian state-sponsored malicious cyber actors." ([Strengthening Cybersecurity of SATCOM Network Providers and Customers | CISA](#))

May 10, 2022 – In testimony to the Senate Armed Services Committee, Director of National Intelligence Avril Haines analyzes why Russia's level of cyber activity in Ukraine has been unexpectedly low.

Chairman Reed: "One other final, final question. Are you surprised that the Russians have not used cyberattacks against third parties or against the United States directly up to this point? I think that was a concern we all had from the beginning of this operation."

Ms. Haines: "I think what we have seen is the Russians have obviously attacked Ukraine, and we have attributed a variety of attacks to them in that context, including, for example, destructive wiper attacks against Ukrainian government websites, DDoS attacks against their financial industry. They also were engaged in attacks intended to get at command-and-control communications in Ukraine during the invasion. That attack had an outsized impact. In other words, we assessed that they intended to focus in on Ukrainian command and control but ultimately they ended up affecting a much broader set of VSATs, essentially, you know, very small terminals outside of Ukraine, including in Europe."

“And yet we have not seen the level of attacks, to your point, that we expected, and we have a variety of different theories for why that might be the case, including the fact that we think that they may have determined that the collateral impact of such attacks would be challenging for them in the context of Ukraine, also that they may not have wished to essentially sacrifice potential access and collection opportunities in those scenarios.

“And then in terms of attacks against the United States, I think they have had a longstanding concern about the potential for escalation in cyber, vis-à-vis the United States. That does not mean that they will not attack at some point, but it has been interesting to see that they have not during this period.” ([OPEN/CLOSED\\* To receive testimony on worldwide threats \(senate.gov\)](#))

May 10, 2022 – A State Department release describing the scope of U.S. government support for Ukrainian cyber activities notes the following:

“The Federal Bureau of Investigation (FBI) has provided direct support to its Ukrainian national security and law enforcement partners, including briefing Ukrainian partners on Russian intelligence services’ cyber operations; sharing cyber threat information about potential or ongoing malicious cyber activity; helping to disrupt nation-state efforts to spread disinformation and target the Ukrainian government and military; and sharing investigative methods and cyber incident response best practices. The FBI also has received threat intelligence and leads from its Ukrainian partners for action using the FBI’s unique investigative and intelligence capabilities. FBI, State, and other U.S. government agencies have also assisted Ukraine with identifying and procuring hardware and software to support network defense.”

“Technical experts funded by the U.S. Agency for International Development (USAID) are providing hands-on support to essential service providers within the Ukrainian government including government ministries and critical infrastructure operators to identify malware and restore systems after an incident has occurred. This support builds on long standing USAID support building cyber resilience among regional utilities, particularly in the energy sector. USAID and the Department of State are also exploring new mechanisms to leverage the services offered by U.S. and Ukrainian cybersecurity service providers to support and reinforce the Government of Ukraine’s own cyber defense efforts.” Furthermore, “USAID has provided more than 6,750 emergency communications devices, including satellite phones and data terminals, to essential service providers, government officials, and critical infrastructure operators in key sectors such as energy and telecommunications.”

“The Department of Energy (DOE) and other interagency partners are working with Ukraine on efforts related to further integrating Ukraine’s electrical grid with the European Network of Transmission System Operators for Electricity (ENTSO-E), including meeting cybersecurity requirements and enhancing the resilience of its energy sector. Full ENTSO-E integration is key to protecting Ukraine’s financial, energy, and national security.” ([U.S. Support for Connectivity and Cybersecurity in Ukraine - United States Department of State](#))



May 10-11, 2022 – Speaking at CYBERUK 2022, Western cybersecurity officials warn about the problems of “cyber vigilantes.” NSA’s Rob Joyce comments: “You want to sit back and root for the folks who are trying to do noble things [in Ukraine] but it is problematic. We are trying to hold bad actors accountable in other nations [and] we have to be good international citizens in the cyber arena.”

Abigail Bradshaw, head of the Australian Cyber Security Centre (ACSC), reveals that the Ukraine war has involved some 300,000 hactivists, a figure that has “taken [us] by surprise.”

Joyce notes that recent events including China’s continuing attacks on American IT systems have finally begun changing intelligence agency attitudes about the need for cyber defense. “We will now do the things that we should have done ten or 20 years ago. The narrative has shifted.”

Drawing some lessons from current conflict, Juhan Lepassaar, executive director of the European Union Agency for Cyber Security notes: “Moving the onus of cyber security from response to prevention is key, as Ukraine’s example shows. The country’s high state of preparedness and resilience have been major factors in its ability to stay online during the war. Another lesson, Lepassaar says, has been “the value of building partnerships early on and making sure you build distributed systems that are difficult to take down and attack.” ([NSA's Rob Joyce: Even the good hactivists are problematic \(newstatesman.com\)](#))

May 12, 2022 – Four Democratic congressional committee chairs send letters to the CEOs of YouTube, TikTok, Twitter, and Meta requesting that they “flag or mark” content on their platforms “containing potential evidence of war crimes and other atrocities” by Russia in Ukraine. The signatories are Reps. Carolyn Maloney, D-N.Y., chair of the Oversight Committee; Gregory Meeks, D-N.Y., chair of the Foreign Affairs Committee; Stephen Lynch, D-Mass., chair of the Oversight and Reform subcommittee on national security; and William Keating, D-Mass, chair of the Foreign Affairs subcommittee on Europe, energy, the environment and cyber. ([Facebook, YouTube and TikTok asked by four House Committee chairs to archive war crime evidence \(nbcnews.com\)](#))

May 13, 2022 — Russian forces physically storm an internet company in Kherson. SSSCIP, the Ukrainian government communications agency, issues a statement shortly afterwards: “This morning, terrorists from the so called Russian Guard invaded the office of Status, a Kherson-based company, and disconnected all the communication equipment. Now they are blackmailing the company’s management and promise to take away all the equipment if those refuse to connect to the Crimean network. That is a gross violation of the international law. We record all such incidents and will use them as evidence in the suits against Russian criminals to be investigated by international competent courts.”

Herb Lin tells CybeScoop: “This is an entirely different kind of cyberattack: This company is not being cyberattacked through the Internet ... It is a cyberattack because its equipment is being commandeered by armed thugs.” He warns of the “potent effect” of this “more forceful” kind of assault, adding, “It’s significant because now Ukrainians can’t get better information from the West. It’s not just adding .ru.

It's taking away .us. and .eu and cutting them off from accurate information.”  
([Invaders use blackmailing and intimidation to force Ukrainian Internet service providers to connect to russian networks \(cip.gov.ua\)](#); [Russians allegedly storm Ukrainian ISP, blackmail it to switch to Russian networks \(cyberscoop.com\)](#))

May 13, 2022 – A *Washington Post* article on Biden administration plans to walk back provisions of NSPM-13 (“United States Cyber Operations Policy,” 2018) mentions the possible implications for Ukraine. The still-classified Trump-era directive reportedly authorizes the Pentagon to override State Department objections to the launch of offensive cyber operations – and even to bypass White House approval. A particular question at issue for diplomats is whether the foreign policy implications of such an operation could be guaranteed a full hearing. “For example: One official pointed to the ongoing war in Ukraine and the prospect that a U.S. cyber operation could escalate tensions. ‘Is the risk really worth the benefit?’ the official asked.” ([The Biden administration is refining a Trump-era cyber order - The Washington Post](#))

May 13, 2022 – An analysis published in *infosecurity* magazine points up one perhaps unanticipated outcome of the war – the decision by many Ukrainians to turn to cryptocurrency once the banks closed and the country ran out of hard currency. “Suddenly, the concept of decentralized finance made sense in a real-world scenario. Central banks aren’t functioning. So, out of cash, how do we pay for things? Crypto is the answer.” ([What the War in Ukraine Means - Infosecurity Magazine \(infosecurity-magazine.com\)](#))

May 16, 2022 – The Killnet group declares cyberwar on 10 countries – the United States, the U.K., Germany, Italy, Latvia, Romania, Lithuania, Estonia, Poland, and Ukraine. Italy comes under special focus after Anonymous Italy began retaliating. That in turn sparks the larger #Anonymous collective to announce it is “officially in cyber war against the pro-Russia hacker group #Killnet.” Killnet is not seen as a highly sophisticated operation, according to analysts. ([Killnet: The Hactivist Group That Started A Global Cyber War \(digitalshadows.com\)](#))

May 18-19, 2022 – Moscow plays host to one of Russia’s largest annual hacker conferences, Positive Hacker Days. This year, some 8,700 people attend the event. A later analysis by the Brookings Institution delves into this year’s event to explore what it shows about the nexus between the country’s nongovernmental actors and the government, particularly the case of conference organizer Positive Technologies. ([PHDays — international forum on applied digital security. Main page](#); [Russia’s largest hacking conference reflects isolated cyber ecosystem \(brookings.edu\)](#))

May 19, 2022 – Mandiant posts a lengthy blog entry focusing on several significant information operations the company has been tracking relating to the Russian invasion of Ukraine. The report identifies a number of active entities in support of the interests of Russia, Belarus, China, and Iran. ([The IO Offensive: Information Operations Surrounding the Russian Invasion of Ukraine | Mandiant](#))

May 19, 2022 – At a meeting of NATO military leaders, the Supreme Allied Commander Transformation, French Air and Space Gen. Philippe Lavigne, comments that after Russia's invasion of Ukraine, the alliance must continue to adapt at many levels: "Transformation is not only technology, it is innovation, it is a mindset change, it is people and their new skills." NATO has to be able to operate in multi-domain operations, namely land, sea, air, space and cyber, and "synchronize with multiple actors, military, governmental, civilian and industry." ([NATO Military Leaders Address Security in Wake of Russian Invasion of Ukraine > U.S. Department of Defense > Defense Department News](#))

May 19, 2022 – The Conti ransomware group shuts its main operational functions, according to Advintel, which reports this "was not a spontaneous decision, instead, it was a calculated move, signs of which were evident since late April." However, the move is actually part of an act of "sleight of hand," Advintel reports, as the group has spent the past two months creating "subdivisions" that were already going online before the shutdown. Hoping to avoid the failures of collectives like REvil and DarkSide, Conti's leaders understood the need to make these new entities seem entirely unconnected to the prior group, in large part because Conti's decision to declare its support for Moscow brought it potentially under the shadow of OFAC sanctions – not to mention a \$10 million State Department bounty (see May 6, 2022, entry). Analysts report that Conti has received "almost no payments" since February. ([DisCONTInued: The End of Conti's Brand Marks New Chapter For Cybercrime Landscape \(advintel.io\)](#))

May 24, 2022 – Google's "[Jigsaw](#)" unit posts an item online describing its past and present activities in Ukraine. For example: "Almost 10 years ago, amidst the Euromaidan protests that would eventually sweep the Yanukovitch government from power, we deployed Project Shield to protect the newspaper Ukrainian Truth." Continuing: "Today, through Google Cloud, Project Shield is once again at work in Ukraine — protecting over 150 sites, including government, newspapers, and NGOs. In the last 5 years, Shield has been deployed to protect more than 2,300 sites in over 140 countries." Google is also making available its "Outline" software to enable people in the region to create the equivalent of virtual private networks. ([A suite of tools to help protect the free and open web | by Jigsaw | Jigsaw | May, 2022 | Medium](#); WaPo, "How Russia's vaunted cyber capabilities were frustrated in Ukraine," June 21, 2022)

May 29, 2022 – A Twitter post claims: "Massive attack carried by @YourAnonSpider against the Belarusian government for their complicity in the Ukraine invasion. All their biggest government websites are #Offline. #Anonymous #OpRussia." A group named Spid3r, affiliated with Anonymous, is credited with the attack. ([Twitter; Anonymous Claims Attacks Against Belarus for Involvement in Russian Invasion of Ukraine - Infosecurity Magazine \(infosecurity-magazine.com\)](#))

May 2022 – Dmytro Dubov, head of Ukraine's International Centre for Defense and Security, publishes a two-part study of "Russia's in Ukraine." Part two is on "The

War in Cyberspace” and presents a succinct description and analysis of Russian operations. Despite a three-fold rise in cyberattacks during the conflict’s first month, Dubov finds the overall threat picture less than dramatic. Russia has used “limited methods” with “limited impact” and faces several long-term challenges. These include a shortage of specialists, a lack of awareness of Russia’s own vulnerabilities, weak operational skills among mid-level specialists, and a potential brain drain (estimating up to a quarter of the country’s cybersecurity specialists have plans to leave). (Dmytro Dubov, “Russia’s in Ukraine: The War in Cyberspace” (Series No. 2)

May 2022 – According to Ukrainian cyber official Dmytro Dubov: “Nearly 40 cybersecurity companies have announced their withdrawal from the Russian market and have suspended service for Russian clients. This presents long-term challenges, as many software or hardware solutions cannot be replaced by Russian-owned technologies (according to Russian specialists, replacement may require 6 to 12 months).” (Dmytro Dubov, “Russia’s in Ukraine: The War in Cyberspace” (Series No. 2)

Late May – Early June 2022 – According to IBM Security X-Force, “X-Force analysts have also identified an ITG23 campaign against Ukraine that likely took place in late May or early June. The campaign used an ISO image file created on May 31 that is very similar to the one described in Campaign #3 from late April [see entry above]. X-Force suggests that the careful selection of certain targets may indicate at a minimum ([Unprecedented Shift: The Trickbot Group is Systematically Attacking Ukraine \(securityintelligence.com\)](#))

Late May 2022 – A new, pro-Ukrainian, anti-Russian, and anti-Belarus group surfaces. “At first glance DUMPS Forum appears to be the same as every other run-of-the-mill *Russian language* cybercriminal forum,” [Digital Shadows](#) writes later [emphasis added]. “At present this forum is open to members without any vetting or registration process, however, there is an ongoing request for an invite system that may become the main method of gaining access if the forum builds its notoriety.” “DUMPS Forum likely has an important role to play in the ongoing Russia-Ukraine war; as a hub for hackers and patriotic cyber threat actors, as a symbol of resistance, and making a demonstrable difference on the cyber battlefield. Any success achieved by DUMPS Forum will however attract unwanted attention; the ban on Russian citizens visiting the forum highlights that the forum is already on the radar of the Russian state. It is also realistically possible that the success of DUMPS Forum may inspire other services looking to play a part in the ongoing conflict.” ([Meet DUMPS Forum: A pro-Ukraine, anti-Russia cybercriminal forum | Digital Shadows](#))

May 30, 2022 – Internet networks such as Skynet and Status Telecom, based in Kherson, unexpectedly shut down. The *New York Times* reports later: “Over the next few days, people’s internet connections were restored, but they were running through a Russian state-controlled telecom company in Crimea, Miranda Media, according to Doug Madory, director of internet analysis at Kentik, a company that measures the performance of internet networks.” The *Times* reports that this is part of Moscow’s



nearly unprecedented “authoritarian playbook” to put Ukrainian territory controlled by Russia “in the grip of a vast digital censorship and surveillance apparatus.” ([How Russia Took Over Ukraine’s Internet in Occupied Territories - The New York Times \(nytimes.com\)](#)); see also [Russia Is Taking Over Ukraine’s Internet | WIRED](#))

End May 2022 – More than 15,000 shipments of Western electronic components have made their way to Russia since the invasion, according to a review of Russian customs records published by Reuters in August. The parts include “microprocessors, programmable chips, storage devices and other items.” “Despite what the West has described as an unprecedented series of strict sanctions against Russia, many commodity electronic components still aren’t subject to export controls. And even if they are, there’s a global galaxy of suppliers and traders in East Asia and other countries that are willing to ship them and are often beyond the control of Western manufacturers.” ([As Russian missiles struck Ukraine, Western tech still flowed \(reuters.com\)](#))

June 2022 – The Center for Strategic & International Studies (CSIS) publishes “Cyber War and Ukraine” by James A. Lewis. It is billed as a “preliminary review of cyber operations in the Ukraine conflict based on publicly available information.” Noting that cyber operations have offered few benefits so far for Russia, the article points up “questions about the balance between defense and offense in cyberspace, the utility of offensive cyber operations, and the requirements for planning and coordination.” ([220616 Lewis Cyber War.pdf \(csis-website-prod.s3.amazonaws.com\)](#))

June 2022 – *Wired* notes: “In June, Russia tightened its laws on “foreign agents,” cracked down further on the use of VPNs, announced a database collecting IMEI codes of mobile phones, told officials not to use foreign video conference software such as Zoom and instant messaging apps, and launched a draft law that would stop foreign software being used in the country’s critical infrastructure by 2025. ([Russia Is Quietly Ramping Up Its Internet Censorship Machine | WIRED](#))

June 2022 – U.K. finance firms are hit five times this month, according to data from the Financial Conduct Authority (FCA). As in March (see entry), some analysts believe the attacks relate to the war in Ukraine, although ransomware motives may also be a factor. ([DDoS Attacks on UK Firms Surge During Ukraine War - Infosecurity Magazine \(infosecurity-magazine.com\)](#))

June 2022 – According to TRM Labs, in a later report on the use of Bitcoin by Russian-based groups to buy military equipment for the war in Ukraine, Romanov Light, a Telegram channel created in April 2020 and credited with raising more than \$174,000 in cryptocurrencies since the start of the war, launches a targeted fundraising campaign on behalf of the Special Rapid Response Unit (“SOBR”), described as an elite Special Forces unit in the Russian military. ([TRM Analysis:](#)

[Crypto Fundraising Groups Supporting Russian Battlefield Efforts | TRM Insights \(trmlabs.com\)](#)

June–July 2022 – *Wired* writes: “Over the last two months, Russian officials have made around half a dozen policy or legal announcements that look to ramp up control over the web and the country’s tech ecosystem. In July, so far, legislators have proposed the creation of a Russian app store that would be installed on new phones and introduced a law that could limit people’s data being moved out of the country. Russia’s parliament also voted to allow people’s biometric data to be gathered from banks and added to one big database. Google has been fined \$374 million for not falling in line, and Apple has been fined for not storing data in Russia.” ([Russia Is Quietly Ramping Up Its Internet Censorship Machine | WIRED](#))

June 1, 2022 – (Date approx.) Elon Musk tells SpaceX staff that the company has delivered 15,000 Starlink satellite communication kits to Ukraine since late February. (<https://twitter.com/i/status/1533408313894912001>; [Elon Musk: SpaceX Has Sent 15,000 Starlink Kits to Ukraine \(businessinsider.com\)](#))

June 1, 2022 – USCYBERCOM Commander Nakasone makes several noteworthy statements in an interview with SkyNews published today:

- That the US has “conducted a series of operations across the full spectrum; offensive, defensive, [and] information operations” in support of Ukraine
  - That “strategic disclosure” (SkyNews phrase) of Russian malign behavior to governments and the public, a tool in U.S. strategy since 2018, has played a big part in American support for Ukraine: “The ability for us to share that information, being able to ensure it’s accurate and it’s timely and it’s actionable on a broader scale has been very, very powerful in this crisis.”
  - That official reports of Russia’s cyber operations against Ukraine have not been exaggerated: “If you asked the Ukrainians, they wouldn’t say it’s been overblown. If you take a look at the destructive attacks and disruptive attacks that they’ve encountered – you wrote about it in terms of the attack on [satellite company] Viasat – this is something that has been ongoing ... And we’ve seen this with regards to the attack on their [Ukraine’s] satellite systems, wiper attacks that have been ongoing, disruptive attacks against their government processes. This is kind of the piece that I think sometimes is missed by the public.”
  - That the Ukrainian response has been impressive: “It isn’t like they haven’t been very busy, they have been incredibly busy. And I think, you know, their resilience is perhaps the story that is most intriguing to all of us.”
  - That all U.S. activities have been lawful and subjected to full civilian oversight.
  - That he is concerned “every single day” about possible Russian cyberattacks against the U.S. and that hunt forward activities are a useful means of self-protection for America and its allies
- ([US military hackers conducting offensive operations in support of Ukraine, says head of Cyber Command | Science & Tech News | Sky News](#))

June 2, 2022 – National Cyber Director Chris Inglis discusses at a public forum some cyber aspects of the war in Ukraine, including the “mystery” of Russia’s apparently modest use of such operations and Ukraine’s talent for cyber defense:

“Why haven’t the Russians been more successful in using cyber against the Ukrainians? Why haven’t they perhaps kind of at least visibly done more kind of outside of that against all the predictions that they would use not just disinformation but cyber broadly to hold not just the Ukrainian society at risk but any of those who would aid and abet them?

“And I think that there are many kind of reasons why we might imagine that it hasn’t been what we expected. One of those that comes foremost to mind is the Ukrainians are actually quite good at cyber defense. They’ve been trained richly by a partner just to the north of them for the last eight years to be good at cyber defense.

“It turns out they are. It turns out that the kind of activities of the private sector and the public sector combined has created a more resilient kind of infrastructure, both in terms of its inherently more resilient and robust, and when we find a flaw in it, we can add scope and scale, deploy patches, or interdict those threats on the fly.

“It turns out the Russians have not been as aggressive in holding things outside of Ukraine at risk, using what we might call cyber kind of offensive methods, as we might have expected. I can only surmise that, you know, some of that is because they’re busy, some of that is because they kind of understand that there are thresholds — they don’t know quite where those thresholds are and they don’t want to cross those — but I’ll leave that to the fullness of time, in terms of how to properly understand that.” ([FDD | Strengthening America’s Cyber Resiliency: A Conversation with the National Cyber Director](#))

June 2, 2022 – WithSecure chief research officer Mikko Hyppönen tells an audience in Helsinki that Russia has been “largely failing” in its cyberattacks on Ukraine. The recent drop in reports of cyber activity between the two combatants is not because of fewer attacks or a lack of trying on Russia’s part. The reason is that “Ukraine has been able to defend itself both in the real world but also in the online world. In fact, I’ll claim that Ukraine is the best country in Europe to defend its networks against governmental attacks from Russia. Why is that? Well, it’s because they’ve been doing it for eight years. They’ve been doing it for real, over and over again.” ([Insight: Russia is ‘failing’ in its mission to destabilize Ukraine’s networks after a series of thwarted cyber-attacks | The Daily Swig \(portswigger.net\)](#))

June 2, 2022 – Germany’s Bundestag committee on the budget approves the creation of a Bundeswehr Special Fund that includes almost 500 million euros for R&D on artificial intelligence. The U.K. initiates a similar strategy for defense, reflecting the sense of urgency sparked by the Ukraine war, according to one analysis.

The same report also notes that “long-standing ethical concerns over the use of AI in warfare have [also] become more urgent as the technology becomes more and more advanced.” Although the private sector has been reluctant in the past to cooperate with the government on matters of warfare, “Silicon Valley is closer to the

world's militaries than ever. And it's not just big companies, either—startups are finally getting a look in, (Bundestag, "Committees approve business plan for special funds," 6-2-22; [Why business is booming for military AI startups | MIT Technology Review](#))

June 2, 2022 – The Legion group, reportedly established by Killnet and sometimes describing itself as Cyber Spetsnaz, launches a campaign to recruit participants in an "elite cyber squad" called Sparta. ([Dark Covenant 2.0: Cybercrime, the Russian State, and the War in Ukraine \(recordedfuture.com\)](#))

Early June 2022 – Russia finally succeeds in reconfiguring networks and rerouting Internet traffic through Crimea to Russia, according to Victor Zhora, deputy head of Ukraine's SSSCIP. Until now, Ukraine ISPs have been able to control the Internet in the country's Russian-occupied territories, he says. "[W]e understand that the objective is to sow disinformation, to sow panic and instability," he tells CyberScoop. ([Mixed results for Russia's aggressive Ukraine information war, experts say \(cyberscoop.com\)](#))

June 4, 2022 – According to TRM Labs, the Russian group Novorossia Aid Coordinating Center (NACC) posts a message on Telegram stating it plans to supply and train Russian-backed forces in Ukraine with drones starting in July, and to donate 15 Mavic 2 and Mavic 3 brand drones. Other organizations are named as participants in the training sessions: the 4th Brigade of the LPR (very likely the Prizrak Mechanized Brigade); an undisclosed Russian Artillery Unit; the Marine Corps Brigade of the Black Sea; and Reservist Units of the LPR. ([TRM Analysis: Crypto Fundraising Groups Supporting Russian Battlefield Efforts | TRM Insights \(trmlabs.com\)](#))

June 5, 2022 – Ukraine's SBU claims it has gained "access to propaganda manuals of Russian special services about 'correct coverage of special operation' in Ukraine," reporting that the materials acknowledge Russia's failure to persuade its population of the need for the war and recommend a variety of new approaches to the task. ([SBU gains access to propaganda manuals of Russian special services about "correct coverage of special operation" in Ukraine \(video\) \(ssu.gov.ua\)](#))

June 6, 2022 – DNI Avril Haines sits for an interview with Michele Fleurnoy at the RSA conference. Discussing Ukraine (15:20–19:14 mark on video), Fleurnoy comments that "one of the things that's been remarkable to watch in the Russia-Ukraine conflict is the speed with which the Intelligence Community has declassified information, shared it with allies and partners to build a common threat picture and really deny President Putin the ability to assert a false narrative ... which is pretty different than how it's worked in the past." She asks Haines to reflect on lessons learned so far in the cyber domain in Ukraine.

Haines (16:20): "Honestly, in many respects my first and best answer is we don't yet know just because the conflict obviously continues, and I think there are still further chapters to be revealed on how this develops. And even with respect to Russia's use of cyber, in many ways I think people didn't see quite the level or scope



of attacks in effect that they expected to see combined with the invasion and yet we're still watching to see how Russia continues in this space. And, of course, we have attributed to Russia a number of attacks that have occurred thus far with respect to Ukraine, targeting Ukraine in particular – you know, their command-and-control, their websites, their emergency response, a variety of things that we've indicated thus far.

"In terms of lessons learned, I think there are a few things. One is ... the degree of sharing that we've done during this whole process has been pretty extraordinary and from my perspective a part of that was because as we entered into this – really the Fall of last year – as we were starting to see the intelligence that indicated that Russia was going to – or was at least very seriously considering an invasion along these lines, we sort of encountered a fair amount of skepticism among folks, and when we explained to our policymakers and our policymakers went to their interlocutors they found that there was a fair amount of skepticism about it.

"And, as a consequence, the president came back to us and said, you know, 'you need to go out and share as much as you possibly can and ensure that folks see what it is that you're seeing, so that we can engage again and perhaps have more productive conversations about how to plan for essentially the potential of a Russian invasion.'

"And, in that process, we did a lot of sharing in this space with partners and allies, and we learned a lot from them in that process, and we also developed mechanisms for sharing that I think will help us in the future. And among the key issues was cyber, right? Like, how would the Russians use cyber? How did we expect them to engage in that in the context of a conflict? What were some of the things that we expected to see? And as the conflict has continued and we've seen attacks like the Viasat attack, for example, that spread into Europe and other things like that, we benefited from the opportunities to share that information as quickly as possible and get it out and then also learn about the impact from these [bases?]. But I would say that we are still looking to see how it is that the Russia cyber story develops over time." ([Rethinking the Cybersecurity Challenge from an IC Perspective - YouTube](#))

June 6-9, 2022 – (Approx.) Also at the RSA Conference, former senior FBI official Shawn Henry tells corporate CISOs "China is absolutely watching what's happening in Russia and Ukraine, what the U.S. is doing or not," and that private firms need to be ready for a possible Chinese invasion of Taiwan. CyberScoop later notes that among the lessons Beijing might be picking up are: S"trike quickly, pick targets that would cripple the enemy early on and rely on attack methods that never have been observed in public." ([The Ukraine war could provide a cyberwarfare manual for Chinese generals eyeing Taiwan \(cyberscoop.com\)](#));

June 7, 2022 – As of this date, Ukraine's IT Army has reportedly conducted DDoS attacks against 662 Russian government and company website targets. ([Cyber-Reports-2022-06-IT-Army-of-Ukraine.pdf \(ethz.ch\)](#))

June 8, 2022 – NSA Cybersecurity Director Rob Joyce tells the RSA Conference in San Francisco that “Russia is in a hybrid war with Ukraine” and that, contrary to assumptions, beyond “kinetic action, what we’ve seen is an enormous amount of cyber activity” consisting of a “multi-pronged-attack and threats.” ([NSA cyber chief says there has been ‘enormous’ amount of hacking in Ukraine war \(scmagazine.com\)](#))

June 8, 2022 – SkyNews posts a lengthy follow-up piece to its interview with Paul Nakasone (June 1). The article reports that the outlet sought a White House comment on the general’s admission about the U.S. conducting offensive cyber operations on behalf of Ukraine: “Responding to whether the offensive cyber operations were contrary to the US position of avoiding direct engagement with Russia, [Press Secretary] Ms Jean-Pierre said: ‘We don’t see it as such. We have talked about this before. We’ve had our cyber experts here at the podium lay out what our plan is. That has not changed. So the answer is, just simply, no.’” ([Ukraine war: US cyber chief on Kyiv’s advantage over Russia | Science & Tech News | Sky News](#))

June 8, 2022 – Exploring a high-profile case of Western assistance to Ukraine, *Politico* publishes an article on “How Elon Musk’s space satellites changed the war on the ground” – by helping Ukrainian drones bomb Russian targets; allowing people isolated near the Russian border to keep in contact with family members; and even enabling President Zelensky to stay current on social media and Zoom with world leaders.

“The strategic impact is, it totally destroyed [Vladimir] Putin’s information campaign,” Brig. Gen. Steve Butow, director of the space portfolio at the Defense Innovation Unit, tells the magazine. “He never, to this day, has been able to silence Zelenskyy.”

The article continues: “The conflict in Ukraine also has provided Musk and SpaceX’s fledgling satellite network with a trial-by-fire that has whetted the appetite of many Western militaries. Commanders have been impressed by the company’s ability, within days, to deliver thousands of backpack-sized satellite stations to the war-torn country and to keep them online despite increasingly sophisticated attacks from Russian hackers.” ([UkraineX: How Elon Musk’s space satellites changed the war on the ground – POLITICO](#))

June 9, 2022 – The head of international information security for the Russian Foreign Ministry, Andrei Krutskikh, issues a statement pointing to circles in the United States and Ukraine as being behind a series of cyberattacks on Russia’s critical infrastructure and state institutions over the previous weekend (June 4-5). He charges that the U.S. is “deliberately lowering the threshold for the combat use” of IT and warns: “The militarization of the information space by the West and attempts to turn it into an arena of interstate confrontation, have greatly increased the threat of a direct military clash with unpredictable consequences.” “Rest assured, Russia will not leave aggressive actions unanswered. All our steps will be measured, targeted, in accordance with our legislation and international law.” His statement, which follows an interview with *Kommersant*, is reported as apparently a response to Gen.

Paul Nakasone's June 1 admission that the U.S. has conducted offensive cyber operations against Russia. ([Russia says West risks 'direct military clash' over cyber attacks | Reuters](#); [Russia escalates threats against West in response to cyberattacks \(cyberscoop.com\)](#); [МИД РФ видит угрозу прямого киберстолкновения с США - Новости - Мир - Коммерсантъ \(kommersant.ru\)](#))

June 14, 2022 – NATO members issue a communiqué following the 30-nation summit in Brussels intended to “open a new chapter in transatlantic relations” in an “increasingly complex” security environment. The document includes a section on cyber threats and notes the endorsement of NATO's Comprehensive Cyber Defence Policy. It declares that the North Atlantic Council will decide case-by-case whether to invoke Article 5. “Allies recognise that the impact of significant malicious cumulative cyber activities might, in certain circumstances, be considered as amounting to an armed attack.” (Brussels Communiqué, 6-14-21)

Mid-June 2022 – Further on the debate on the link between cyber and conventional military conflict, two scholars lay out their current findings from the Ukraine war to argue that the Kremlin has used the two capabilities independently of each other. “As our theory explains, traditional military operations are the most effective method of occupying territory, capturing resources, attriting [sic] an enemy's conventional military capabilities, and terrorizing populations. Cyber operations, on the other hand, are most consistently effective in gathering intelligence, stealing technology, and winning public opinion and diplomatic debates. As a result, conflict in cyberspace has more typically been about winning information contests than it has been about augmenting or replacing the physical aspects of a conventional war, at least directly ... [B]ecause of the unique objectives that each mode serves, they can instead act to indirectly substitute for one another. Existing evidence suggests that Russia has used its information campaigns to indirectly substitute for conventional conflict in the longer term, especially given that Moscow seems to have expected the war to be short.”

On the specific question of why Russia has not done more in terms of offensive cyber operations against Ukraine's critical infrastructure, the authors offer this explanation: “The war in Ukraine is fundamentally about territory and physical control. Cyberspace can do little to capture a nation. It can, however, serve as a vehicle through which one can attempt to capture the hearts and minds of a people. But to compete in this manner, both sides must maintain access to the internet.” ([Why Cyber Dogs Have Yet to Bark Loudly in Russia's Invasion of Ukraine - Texas National Security Review \(tnsr.org\)](#))

June 15, 2022 – The head of France's Space Command, Maj. Gen. Michel Friedling, expresses the view that Russia signaled its intentions toward Ukraine before launching its ground assault. “What Ukraine has shown us well is that things will begin in [the] cyber and space domain before beginning on the ground ... The cyberattack against Viasat was done the day before the beginning of the ground invasions. This is very significant. And this is very interesting. This is a big lesson. I would say it's something we were thinking but now it's real.” The previous November 15, Russia

reportedly conducted a weapon test that destroyed one of its own satellites, an act Friedling said proved that Russia was “ready to deny us [sic] space capabilities to other players, ... even if it denies to [Russia, themselves] the use of space capabilities.” ([How Russia telegraphed invasion of Ukraine in space and online \(defensenews.com\)](https://www.defensenews.com/defense/2022/06/15/russia-satellite-test/))

Mid-June 2022 – According to IBM Security X-Force, “X-Force analysts in mid-June identified a suspicious CobaltStrike sample using ITG23’s Tron crypter, suggesting a relationship to ITG23 or one of its partners or affiliates. CERT-UA a few days later released a report indicating that this CobaltStrike sample was used in recent phishing attacks against “critical infrastructure facilities of Ukraine.” To deliver the payload, the attacker used emails purporting to be from the ... ‘State Tax Service of Ukraine’ .... The email and document lure contain information about requirements to pay taxes in Ukraine. Of note, the text in the document lure is identical to that posted on this web page about Ukrainian tax requirements ... Of note, the SSL Public Key embedded in this Beacon is identical to the one in the Beacon used in Campaign #5 [see Late May – Early June entry above], indicating that these two Beacons can be traced back to the same CobaltStrike Team Server installation.” ([Unprecedented Shift: The Trickbot Group is Systematically Attacking Ukraine \(securityintelligence.com\)](https://www.securityintelligence.com/news/2022/06/15/unprecedented-shift-the-trickbot-group-is-systematically-attacking-ukraine/))

June 15, 2022 – Rear Adm. TJ White (Ret.), former head of the U.S. Cyber National Mission Force, tells a public audience that Russian information operations have been continuous but have been largely frustrated by the wide availability of the Starlink satellite internet system and many Ukrainians’ access to virtual private networks (VPNs). ([Mixed results for Russia's aggressive Ukraine information war, experts say \(cyberscoop.com\)](https://www.cyberscoop.com/tj-white-starlink-ukraine/))

June 17, 2022 – President Putin’s speech at the St Petersburg International Economic Forum is delayed, allegedly due to a cyberattack. ([Russia-Ukraine latest: Russia ‘overwhelmingly’ striking civilians | Russia-Ukraine war News | Al Jazeera](https://www.aljazeera.com/news/2022/6/17/russia-ukraine-latest-russia-overwhelmingly-striking-civilians/))

June 21, 2022 – An op-ed by David Ignatius in *The Washington Post* makes various points about the cyber dimension of the war in Ukraine. Among them: “The close partnerships that have emerged between U.S. technology companies and Western cybersecurity agencies is one of the unheralded stories of the war. The public-private rift in the tech world that followed Edward Snowden’s revelations in 2013 appears largely to be over — because of the backlash against Russia’s attacks on the 2016 and 2020 U.S. presidential elections and, now, its unprovoked invasion of Ukraine.” Ignatius also notes Ukraine’s “digital savvy” as a factor in its favor after years of hacking and even fraudulent activities, plus its experiences over eight years of war with Russia. He adds that Russia’s reliance on Western technology for cyberattacks could backfire “in ways that persist for years.” (WaPo, “How Russia’s vaunted cyber capabilities were frustrated in Ukraine,” June 21, 2022)



June 22, 2022 – Microsoft publishes “Defending Ukraine: Early Lessons from the Cyber War” offering a current assessment of Russia’s operations, Ukraine’s ability (with outside help) to deflect attacks, and a series of conclusions that derive from the first four months of the war. Among many other data points, the report counts 128 Russian network intrusions in 42 countries during this period. Government agencies were targeted 48% of the time, IT sector enterprises 20%, critical infrastructure organizations 19%, and NGOs 12%. Microsoft assesses a “success rate” of 29% though it states this may be an understatement. ([Defending Ukraine: Early Lessons from the Cyber War \(microsoft.com\)](#))

Shortly after the report’s release, CyberScoop posts an article noting that “serious questions and concerns” have been raised about the report. “In total, CyberScoop spoke with a dozen prominent cybersecurity threat analysts, executives, military cyber practitioners and scholars who all criticized Microsoft for publishing a report that didn’t contain either the technical underpinning or evidence to back up its points. What’s more, they said, it didn’t meet basic standards of academic research that even most tech companies adhere to when producing similar reports on nation-state or criminal cyber threat activities.” ([Cybersecurity experts question Microsoft's Ukraine report \(cyberscoop.com\)](#))

June 22, 2022 – The IT Army of Ukraine and its implications for future cyber conflict are the subject of a detailed study published by the Center for Security Studies, ETH Zurich. Author Stefan Soesanto maintains that the IT Army’s “organizational setup and operational impact will likely inform the art of cyber and information warfare in future conflicts.” He describes a group that “has rapidly evolved from mere defacements of Russian websites during the first days of the invasion, to sophisticated espionage campaigns, to the first destructive offensive cyber operation – targeting a civilian video platform – in early May 2022.” If the trend continues, “Russian defenders will highly likely face a variety of experimental cyber ops that will try to produce more and more severe impacts and longer lasting effects.” He concludes that the group “likely maintains deep links to – or largely consists of – the Ukrainian defense and intelligence services,” something Ukraine authorities have denied.

The IT Army’s campaign presents a glimpse of what the future of cyber warfare looks like while also raising important questions, including normative ones. “Overall, both Kyiv and the Ukrainian IT community at large have shown the world what digital diplomacy on steroids looks like,” but at the same time “their conduct has collapsed entire pillars of existing legal frameworks regarding norms and rules for state behaviour in cyberspace and has taken apart the illusion of separating the defense of Ukraine from Ukrainian companies and citizen living abroad.” Soesanto reproaches EU and NATO member states who “have equally failed to adapt to – or even grasp – what the IT Army really is,” dismissing it as “just a collection of random volunteers conducting meaningless DDoS attacks against Russian websites.” He warns: “For better or worse, continuing to ignore the essence of the IT Army will wreak havoc on the future stability of cyberspace and with it the national security landscape in Europe and beyond.” ([Cyber-Reports-2022-06-IT-Army-of-Ukraine.pdf \(ethz.ch\)](#); [Twitter](#))

June 27, 2022 – The Russian hacker group Killnet claims responsibility for what are described as DDoS attacks against Lithuanian transport and media websites along with the tax service and other state entities. Killnet says it is to retaliate for the blocking of goods into Kaliningrad. ([Could the Russian cyber attack on Lithuania draw a military response from NATO? | World News | Sky News](#))

June 27, 2022 – After Russian missiles today hit the Kremenchuk shopping mall, Russian search engine Yandex reportedly provides returns on searches that only present the official Kremlin line on the attack, according to a former Yandex official quoted by BBC News. It is seen as an example of widespread attempts since the Ukraine invasion to block access to independent media on the Internet in Russia. ([Ukraine war: Russians kept in the dark by internet search - BBC News](#))

Late June 2022 – Pro-Russia hackers NoName057(16) and Killnet jointly carry out several DDoS attacks against government websites in Italy, Romania, Germany, Norway, Lithuania, the Czech Republic and Latvia, according to cybersecurity experts. ([Pro-Kremlin hackers target Latvia's parliament after declaring Russia a sponsor of terrorism - The Record by Recorded Future](#))

June 28, 2022 – According to TRM Labs, a Telegram post for Task Force Rusich, described as a neo-Nazi Russian paramilitary group sanctioned by the U.S. Treasury's Office of Foreign Assets Control (OFAC), confirms the purchase of numerous pieces of radio and other equipment for use by Russia-backed forces in Ukraine. The group is one of several TRM Labs is tracking that uses Bitcoin in its efforts. "Task Force Rusich maintains at least 14 addresses across 7 different blockchains, and benefits from message amplification within other pro-Russian Telegram channels. The group has received over \$144,000 in cryptocurrency since the start of the invasion," TRM Labs reports later. ([TRM Analysis: Crypto Fundraising Groups Supporting Russian Battlefield Efforts | TRM Insights \(trmlabs.com\)](#))

June 29, 2022 – The North Atlantic Council issues the Madrid Summit Declaration after meeting in the Spanish capital. The declaration features an announcement of plans to expand civil-military partnerships and build a "virtual rapid response cyber capability" using lessons learned from the Ukraine war to confront threats from various sources including China. The United States says it will provide "robust" resources for the effort. ([NATO - Official text: Madrid Summit Declaration issued by NATO Heads of State and Government \(2022\), 29-Jun.-2022; NATO to create cyber rapid response force, increase cyber defense aid to Ukraine - CyberScoop; US cyber squad boosts Lithuanian defenses amid Russian threat \(airforcetimes.com\); US seeking to understand Russia's failure to project cyber power in Ukraine \(defensenews.com\)](#))

June 29, 2022 – At Madrid, NATO also issues a new "Strategic Concept" that includes the following passage on cybersecurity:

“25. Maintaining secure use of and unfettered access to space and cyberspace are key to effective deterrence and defence. We will enhance our ability to operate effectively in space and cyberspace to prevent, detect, counter and respond to the full spectrum of threats, using all available tools. A single or cumulative set of malicious cyber activities; or hostile operations to, from, or within space; could reach the level of armed attack and could lead the North Atlantic Council to invoke Article 5 of the North Atlantic Treaty. We recognise the applicability of international law and will promote responsible behaviour in cyberspace and space. We will also boost the resilience of the space and cyber capabilities upon which we depend for our collective defence and security.” (“NATO 2022 Strategic Concept,” June 29, 2022)

June 29, 2022 – After declaring it would not allow sanctioned goods to transit to Kaliningrad, Lithuania is targeted by an unprecedented number of cyber attacks, according to the country’s defense minister, Arvydas Anusauskas. ([Lithuania Faces ‘Intense’ Cyber Attack Amid Kaliningrad Standoff - Bloomberg](#))

June 29, 2022 – Norway’s National Security Authority reveals several organizations in the country have been hit briefly by DDoS attacks, which Bloomberg attributes to KillNet. Norway recently announced it would block shipments of sanctioned materials headed for Russia. ([Russian Hacker Group Killnet Targets Norway’s Public Service Websites - Bloomberg](#))

June 29, 2022 – An analysis posted on OODA LOOP reviews “Lessons on the Future of Cyberwar from Russia.” Among other conclusions about Russia’s operations: “While cyber attacks continue, they seem to be less of a factor and have created less of an impact the more Russian forces battle for territory. In fact, Russia appears to have backed away from relying on cyber attacks against critical civilian infrastructures in favor of using conventional strikes, intimating that kinetic weapons and not cyber ones are more preferable to adversely affect these targets. This indicates that while cyber attacks may inflict fear in a populace, they are not seen as a dependable means to achieve a desired tactical military outcome, most likely due to their unpredictability and their tendency to escape the network boundaries of the specific target. At least for the past four months, Russia seems to be using cyber attacks in a supportive, secondary role, which may be a result of how the military engagement has unfolded, though a full accounting won’t be fully understood until long after the conflict has been resolved.

“Therefore, looking at how Russia has implemented cyber operations in Ukraine, lack of cyber impact may not be the fault of the use of cyber weaponry as the strategy in which it was incorporated.” ([OODA Loop - Lessons On The Future of Cyberwar From Russia](#))

June 30, 2022 – The State Service of Special Communications and Information Protection of Ukraine logs 796 cyberattacks against the country in the first four months of the war. Most of the incidents involve information gathering (242) followed by malicious code (192). “Enemy hackers keep attacking Ukraine. While the intensity of cyberattacks

has not decreased since the beginning of full-scale Russian invasion, their quality is declining. The Ukrainian government and local authorities, military, finance and energy sectors remain the major targets. Transport infrastructure and telecommunications also remain within the cybercriminals' sight." ([Four Months of War: Cyberattack Statistics \(cip.gov.ua\)](#))

June 30, 2022 – NATO launches the Innovation Fund, billed as the world's first multi-sovereign venture capital fund. "This fund is unique," Secretary General Jens Stoltenberg asserts. Over the next 15 years, it "will help bring to life those nascent technologies that have the power to transform our security in the decades to come." According to a NATO statement, "The Fund will invest 1 billion euros in early-stage start-ups and other venture capital funds developing dual-use emerging technologies of priority to NATO. These include: artificial intelligence; big-data processing; quantum-enabled technologies; autonomy; biotechnology and human enhancement; novel materials; energy; propulsion and space." The Fund will complement NATO's existing Defence Innovation Accelerator for the North Atlantic (DIANA), which aims to promote security-related dual-use emerging technologies. (NATO, "NATO launches innovation fund," 6-30-22)

Mid-2022 – At this stage of the conflict in Ukraine, DDoS attacks remain the most often used weapon on both sides, according to NETSCOUT Systems. DDoS attacks reached 6,019,888 in the first six months of the year. Richard Hummel, threat intelligence lead at the company, comments in a later report: "In the first half of 2022, attackers conducted more pre-attack reconnaissance, exercised a new attack vector called TP240 PhoneHome, created a tsunami of TCP flooding attacks, and rapidly expanded high-powered botnets to plague network-connected resources. In addition, bad actors have openly embraced online aggression with high-profile DDoS attack campaigns related to geopolitical unrest, which have had global implications." A later NETSCOUT report concludes: "The findings demonstrate how sophisticated cybercriminals have become at bypassing defenses with new DDoS attack vectors and successful methodologies." ([Adversaries Continue Cyberattack Onslaught with Greater Precision and Innovative Attack Methods According to 1H2022 NETSCOUT DDoS Threat Intelligence Report | NETSCOUT](#))

Summer 2022 – According to European cybersecurity firm Thales, "In the summer of 2022, there were almost as many conflict-related incidents in EU countries as there were in Ukraine (85 versus 86)." ([From Ukraine to the whole of Europe: cyber conflict reaches a turning point | Thales Group](#))

July 2022 – Sometime this month, a "hunt forward" team from the U.S. Cyber National Mission Force returns from a mission in Croatia. On August 18, 2022, USCYBERCOM releases a statement about the operation. ("[Partnership in Action": Croatian, U.S. cyber defenders hunting for malicious actors > U.S. Cyber Command > News; U.S. Cyber Command completes defensive cyber mission in Croatia \(cyberscoop.com\)](#)")



July 2022 – According to a later Radware report, “In July, threat group NoName057(16) quietly launched a crowdsourced botnet project named 'DDOSIA.' The project, similar to the pro-Ukrainian Liberator by disBalancer and the fully automated DDoS bot project by the IT ARMY of Ukraine, leverages politically-driven hacktivists willing to download and install a bot on their computers to launch denial-of-service attacks. Project DDOSIA, however, raises the stakes by providing financial incentives for the top contributors to successful denial-of-service attacks.” ([Project DDOSIA Russia's answer to disBalancer | Radware](#))

July 2022 – A study, “What Makes Ukraine Resilient in the Asymmetric War?,” by Oksana Huss theorizes that the answer to the question lies in the country’s “culture of collaborative governance and participatory democracy, underpinned by the use of digital media.” Among specific explanations is the nature of Ukraine’s “evolving participatory democracy” which features citizen demands for greater influence on politics that emerged from the Revolution of Dignity in 2013-2014 and prompted reforms affecting decentralization, anti-corruption, and other societal norms. “In addition, digital transformation of the country enabled coordination of collaborative governance by means of e-democracy tools, while extensive implementation of e-governance tools increased efficiency of public services.” ([QM 1-2022 Huss - What Makes Ukraine Resilient in the Asymmetric War? | KHK/GCR21](#))

July-August 2022 – U.S.-sponsored, online psychological operations are exposed when Twitter and Meta remove a series of accounts on grounds of violating terms of service. The two social media platforms provide related data portions to Graphika and the Stanford Internet Observatory (SIO) for analysis. Their joint investigation discovers an “interconnected web of accounts on Twitter, Facebook, Instagram, and five other social media platforms that used deceptive tactics to promote pro-Western narratives in the Middle East and Central Asia. The platforms’ datasets appear to cover a series of covert campaigns over a period of almost five years rather than one homogeneous operation.” Ukraine is a focus of some of these activities. ([Unheard Voice: Evaluating five years of pro-Western covert influence operations \(stanford.edu\)](#))

July 1, 2022 – DTEK, described as Ukraine’s largest private energy investor, reports a cyberattack on the group’s IT infrastructure, which it attributes to the Russian Federation. Ukrainian cyber official Viktor Zhora later cites the incident as an example of Russian actions that Ukraine believes constitute war crimes because they target civilian facilities. ([Enemy launches hacker attacks on the power system — DTEK; Kyiv argues Russian cyberattacks could be war crimes – POLITICO](#))

July 1, 2022 – UNITED24, President Zelenskyy’s global fundraising platform, along with the General Staff of the Armed Forces and the Ministry of Digital Transformation, launch an “Army of Drones” campaign to buy, maintain, and train pilots for a fleet of UAVs. The initial goal is to buy 200 units to provide constant monitoring Ukraine’s 2470 km frontline. The government sends out a worldwide appeal to “Dronate!” ([Ukraine Raises an Army of Drones \(u24.gov.ua\)](#))

July 7, 2022 – IBM Security X-Force reports evidence that the “Trickbot group” (Conti group) “has been systematically attacking Ukraine since the Russian invasion — an unprecedented shift as the group had not previously targeted Ukraine.” The report itemizes half a dozen campaigns between mid-April and mid-June of 2022 that deployed IcedID, CobaltStrike, AnchorMail, and Meterpreter. The authors report that “Russian-speaking criminal underground communities have long generally discouraged if not outright banned going after former Soviet countries and—while not relevant to Ukraine—members of the Commonwealth of Independent States (CIS).” Reasons given include a desire “to avoid creating victims in malware operators’ countries of residence, in large part to avoid antagonizing law enforcement,” and to foster “Russian-speaking criminal cooperation based on a shared sense of us-versus-the-rest solidarity.” ([Unprecedented Shift: The Trickbot Group is Systematically Attacking Ukraine \(securityintelligence.com\)](#))

July 7, 2022 – An article from the Washington Post’s The Cybersecurity 202 discusses today’s IBM Security X-Force report about Trickbot, adding comments from other analysts with somewhat different takes on the issue. The article offers several “caveats” about IBM’s conclusion that the ransomware distributor is working on behalf of the Kremlin, but acknowledges the report presents “a potentially major development in the murky world of ransomware gangs.” In short, the implication of “a major group carrying water for a government’s war objectives is major new territory,” the author concludes. ([Trickbot may be carrying water for Russia - The Washington Post](#))

July 7, 2022 – KillNet implements a DDoS attack on Congress.gov, administered by the Library of Congress, cutting public access for roughly two hours. ([Pro-Russian cybercriminals briefly DDoS Congress.gov \(cyberscoop.com\)](#))

July 7, 2022 – Cloudflare reports on DDoS trends in Ukraine and Russia for the second quarter of 2022:

- “The war on the ground is accompanied by attacks targeting the spread of information.
- “Broadcast Media companies in the Ukraine were the most targeted in Q2 by DDoS attacks. In fact, all the top five most attacked industries are all in online/Internet media, publishing, and broadcasting.
- “In Russia on the other hand, Online Media drops as the most attacked industry to the third place. Making their way to the top, Banking, Financial Services and Insurance (BFSI) companies in Russia were the most targeted in Q2; almost 45% of all application-layer DDoS attacks targeted the BFSI sector. Cryptocurrency companies in Russia were the second most attacked.” ([DDoS attack trends for 2022 Q2 \(cloudflare.com\)](#))

July 8, 2022 – The Defense Department announces authorization of the fifteenth Presidential Drawdown of security assistance for Ukraine since August 2021. It is valued at up to \$400 million and brings the total U.S. commitment under President

Biden to approximately \$8 billion. ([\\$400 Million in Additional Security Assistance for Ukraine > U.S. Department of Defense > Release](#))

July 10, 2022 – Anonymous Russia carries out its first attack since launching its own Telegram group. ([Anonymous Russia: Analysis of Threat Actors in Ukraine-Russia War \(threatmon.io\)](#))

July 11, 2022 – Reflecting growing public interest in (and experts' concern over) the role of hacktivists, an article by *The Record* profiles Nikita Knysh, a 31-year-old former employee of Ukraine's SBU, who has a YouTube channel and a website called [HackYourMom Academy](#), which include tutorials on what *The Record* calls "the basics of digital guerilla warfare." ([How one Ukrainian ethical hacker is training 'cyber warriors' in the fight against Russia - The Record by Recorded Future](#))

July 11, 2022 – A published article discusses the long-standing issue of cybersecurity insurance in the wake of the Ukraine war, noting that there is now a greater focus on systemic cyber risk and the risk to critical infrastructure. According to CyberScoop, "The challenge has policymakers wondering if and when the government should intervene with its own form of insurance." The article quotes a GAO report: "The Department of the Treasury's Federal Insurance Office (FIO) and the Department of Homeland Security's Cybersecurity and Infrastructure Security Agency (CISA) both have taken steps to understand the financial implications of growing cybersecurity risks. However, they have not assessed the extent to which risks to critical infrastructure from catastrophic cyber incidents and potential financial exposures warrant a federal insurance response." ([The cyber insurance market has a critical infrastructure problem \(cyberscoop.com; GAO, "Cyber Insurance: Action Needed to Assess Potential Federal Response to Catastrophic Attacks," June 2022\)](#))

July 11, 2022 – National security advisor Jake Sullivan discloses that Iran is getting ready to provide "up to several hundred" drone UAVs to Russia, "including weapons-capable UAVs on an expedited timeline." He cites it as an example of "how Russia is looking to [other] countries" for help in Ukraine. ([Iran to send hundreds of drones to Russia for use in Ukraine, U.S. says - The Washington Post](#))

July 12, 2022 – Germany announces it will adopt new measures to upgrade its cyber position. Among the steps will be promoting cyber resilience within small-to-medium-sized enterprises that are part of the country's critical infrastructure, installation of a secure central video conferencing system for the federal government, a clearinghouse for information exchange between state and federal agencies, and modernizing the IT infrastructure of the country's domestic intelligence agency and police. Interior Minister Nancy Faeser noted: "The sea change we are facing in view of the Russian war of aggression against Ukraine requires a strategic repositioning and significant investment in our cybersecurity." ([Germany bolsters defenses against Russian cyber threats | News | DW | 12.07.2022](#))

July 12, 2022 – Lithuania’s Vice Minister of National Defense Margiris Abukevičius tells Žinių radio that despite the large number of cyberattacks against state institutions and private enterprises in his country recently their impact has not been significant and the number of failed attacks has far outnumbered the successful ones. “The sky is not really falling,” he says. He argues that giving airtime to these events only aids Russia’s objectives of showing Lithuania and other countries as paying for their actions (creating “success stories that don’t exist”) and raising tensions inside Lithuania. ([Viceministras kibernetinėmis atakomis siekiama viešumo, kelti įtampą \(delfi.lt\)](#))

July 14, 2022 – Yurri Shchychol, head of Ukraine’s SSSCIP, gives a lengthy and detailed interview to Kenneth R. Rosen in *Politico* about Ukraine’s efforts to wage the “first cyber world war” against Russia. Among other topics, he discusses the in-depth coordination his government has had with U.S. and EU officials “responding to cyberattacks while sharing with international allies his insights into strategies used by Russian hackers.”

Shchychol offers insights about the unusual nature of the conflict: “This is the first time in the history of Ukraine, for sure, probably in the world, when the private sector, the cyberprofessionals, are not only doing what they can — professionally defending the cyberspace of their country — but they are also willing to defend it by any means. What you’re referring to is an army currently comprised of more than 270,000 volunteers who are self-coordinating their efforts and who can decide, plan and execute any strikes on the Russian cyber infrastructure without even Ukraine getting involved in any shape or form. They do it on their own. ¶ Other cybersecurity experts, under the guidance of my State Service, have been helpful in providing consultations to government institutions as to how to properly arrange the cybersecurity efforts, especially in the energy sector and critical infrastructure sites. That’s probably the reason none of the cyberattacks that were carried out in the past four months of this invasion has allowed the enemy to destroy any databases or cause any private data leakage.”

Shchychol says the most useful cyber-related equipment Ukraine has received from the U.S. have been 10,000 Starlinks terminals (“the most helpful so far”) for repairing or replacing crippled financial, healthcare, and other infrastructure in local communities; servers and mobile data centers that have allowed state institutions rapidly to back up critical data; and free access to prohibitively expensive software and technologies provided by private industry, such as Amazon’s cloud services. ([The Man at the Center of the New Cyber World War - POLITICO](#))

July 15, 2022 – Symantec begins observing the delivery of information-stealing malware to networks in Ukraine by Shuckworm (Gamaredon, Armageddon, Actinium, Primitive Bear). The activity continues at least until August 8, according to Symantec’s Threat Hunter Team. Shuckworm has been tied to a unit of Russia’s FSB in Crimea. (<https://symantec-enterprise-blogs.security.com/blogs/threat-intelligence/russia-ukraine-shuckworm>)



July 17, 2022 – Volodymyr Zelensky announces his decision to “suspend” Ukraine’s prosecutor general, Iryna Venediktova, and the head of the Security Service of Ukraine (SBU), Ivan Bakanov. Soon after, Zelensky makes clear the two are to be fired, which Parliament approves on July 19. Explanations vary from the desire to put in place more experienced people to the need to address intelligence lapses under Bakanov and apparent corruption by Venediktova. ([Actions and inaction of every official in the security sector and in the law enforcement agencies will be evaluated - address by the President of Ukraine — Official website of the President of Ukraine](#); [Zelensky Fires His Prosecutor General and Intelligence Chief - The New York Times \(nytimes.com\)](#); [Ukraine's Parliament Approves Firing Of Top Prosecutor, Head Of Security Service \(rferl.org\)](#))

July 17, 2022 – The National Agency for Information Society (AKSHI) of Albania announces the country is under a major cyberattack from somewhere outside its borders. ([bne IntelliNews - Russia blamed for wave of hacker attacks in Southeast Europe](#))

July 18, 2022 – A “wide and complex” cyberattack forces Albania’s government and several public institutions to take down their websites. A government statement says the “method used by the hackers was identical with last year’s attacks seen in the international cyberspace,” including in Ukraine. ([Cyberattack blocks Albania's public online services - The Washington Post](#))

July 18, 2022 – The magistrate court of the Tagansky district of Moscow fines Google roughly \$374 million for its “repeated failure” to deal with “prohibited content.” According to a government press release, the court “considered the administrative protocol of Roskomnadzor [Federal Service for Supervision of Communications, Information Technology and Mass Media] against the American IT corporation Google LLC for violating the procedure for restricting access to information recognized as prohibited.

“In particular, Google-owned video hosting YouTube has not restricted access to a number of materials containing prohibited content within the established period:

- fakes about the course of a special military operation in Ukraine, discrediting the Armed Forces of the Russian Federation;
- Materials promoting extremism and terrorism;
- materials promoting an indifferent attitude to the life and health of minors;
- information with calls, including to minors, to participate in unauthorized mass actions.

“For repeated failure to remove prohibited materials, the court imposed a fine of 21,077,392,317.8 rubles on Google, calculated on the basis of the company's annual Russian turnover.” (

July 19, 2022 – Google’s Threat Analysis Group (TAG) posts the following report: “Turla, a group publicly attributed to Russia’s Federal Security Service (FSB), recently hosted

Android apps on a domain spoofing the Ukrainian Azov Regiment. This is the first known instance of Turla distributing Android-related malware. The apps were not distributed through the Google Play Store, but hosted on a domain controlled by the actor and disseminated via links on third party messaging services. We believe there was no major impact on Android users and that the number of installs was miniscule.

“The app is distributed under the guise of performing Denial of Service (DoS) attacks against a set of Russian websites. However, the 'DoS' consists only of a single GET request to the target website, not enough to be effective. The list of target websites for the app can be seen in the CyberChef recipe [here](#).”

This TAG report also gives details on the following activities relating to Ukraine: the Follina vulnerability (exploited by GRU actors APT28 and Sandworm as well as another group known as UAC-0098), Ghostwriter/UNC1151 (attributed to Belarus), COLDRIVER (Russia-based, also known as Callisto), and an entity tracked as UAC-0056 (which sent over 4,500 emails in two days using compromised regional prosecutors’ addresses and delivering Cobalt Strike via malicious Excel documents). ([Continued cyber activity in Eastern Europe observed by TAG \(blog.google\)](#))

July 19, 2022 – The EU denounces the most recent instances of “Russia’s unprovoked and unjustified military aggression against Ukraine.” “The latest distributed denial-of-service (DDoS) attacks against several EU Member States and partners claimed by pro-Russia hacker groups are yet another example of the heightened and tense cyber threat landscape that EU and its Member States have observed. We strongly condemn this unacceptable behaviour in cyberspace.” (Declaration by the High Representative on Behalf of the European Union, 7-19-22)

July 19, 2022 – USCYBERCOM head Paul Nakasone backs up comments made on June 1 (see entry above) about what his command has been doing in connection with Ukraine. Speaking at the International Conference on Cyber Security at Fordham University, he says: “We do three things at U.S. Cyber Command: We defend the Department of Defense’s networks, data and weapons systems. We defend the nation’s cyberspace with a series of interagency partners. And we provide support to joint force commanders like U.S. European Command. So we deny, degrade and disrupt. Being able to detect, defend, disrupt and deter, these are all things that we do in the course of our operations,” he said. “My comments stand in that in terms of what we’re doing, [which] obviously includes a variety of those things to deny, degrade and disrupt. I think this is exactly what we should expect out of U.S. Cyber Command and how we move forward.”

Nakasone adds other comments, for example, that there has been a drop in ransomware attacks, that Russian entities are “much more focused on activities related to Ukraine,” and that there has been a rise in the use of wiper malware. ([Cyber Command chief stands by comments on 'offensive' operations against Russia - The Record by Recorded Future](#))

July 19, 2022 – Speaking at the same conference as Paul Nakasone (see entry above), FBI Director Christopher Wray that the Bureau is seeing a continuation of ransomware attacks against almost every critical infrastructure sector in the United States, albeit with a mix of motives. “Ransomware itself is evolving. It used to be that a bad actor was only a cybercriminal and was only trying to lock up your system for money. Now, two things have changed. Sometimes the ransomware actor isn’t a cybercriminal, it’s a nation-state with a different motive in mind.” He notes a growing trend across the board of a “blended threat” where governments and cybercriminals collaborate. “Nation-state actors now also moonlight and make money on the side as cybercriminals. And nation-states now use cybercriminal tools like ransomware to look like their cybercriminals and not nation-states. All this is happening more and more.” ([Cyber Command chief stands by comments on 'offensive' operations against Russia - The Record by Recorded Future](#))

July 19, 2022 – Exploring the role of cyber sabotage in war against the backdrop of Ukraine, an academic expert notes: “After years of speculation about hybrid warfare and grey-zone tactics, Russia has reverted to form. Its offensive cyberspace operations have been particularly marginal to its conventional military effort. Open sources suggest that Russia has rarely used destructive malware since the February invasion. Over the same period it fired millions of bullets, artillery shells, and rockets, with devastating effect. As Michael Kofman put it, ‘This is a heavy metal war.’

“This has surprised many observers, who thought the war would follow a different path ... It’s easy to see the allure of such a concept, though ... the technical demands are quite high. Nonetheless, Russian military doctrine stresses the importance of information dominance, and analysts have spent years sounding the alarm about the potential for large-scale digital disruption in the event of war. Instead, most Russian efforts appear to be related to espionage and propaganda, with only a smattering of sabotage.” ([Sabotage and War in Cyberspace - War on the Rocks](#))

July 19, 2022 – An analysis published in *Forbes* foresees the emergence of a “new Cold War” in the aftermath of the Ukraine crisis, one that “will likely be fought in cyberspace.” Features will include ransomware carried out by threat actors with ties to nation-states; campaigns on multiple fronts, including the likes of Turkey and Brazil as participants; cyber espionage as the “shortest route to an economic, military or political advantage;” and stealth attacks against infrastructure. ([Why A Second Cold War Will Likely Be Fought In Cyberspace \(forbes.com\)](#))

July 19, 2022 – Palo Alto Networks Unit 42 reports that hackers from APT29 have been using DropBox, Google Drive, and other trusted storage services to hide their operations. “The latest campaigns conducted by an advanced persistent threat (APT) that we track as Cloaked Ursa (also known as APT29, Nobelium or Cozy Bear) demonstrate sophistication and the ability to rapidly integrate popular cloud storage services to avoid detection.” Unit 42 says the most recent targets have been Western diplomatic missions between May and June through the use of phishing

documents with a link to a malicious HTML file called EnvyScout. ([Cloaked Ursa \(APT29\) Hackers Use Trusted Online Storage Services \(paloaltonetworks.com\)](#))

July 19, 2022 – Ukraine’s SBU announces it has shut down an illegal crypto mining center in the Kharkiv region. The farm has reportedly been consuming thousands of dollars’ worth of unpaid electricity. Bitcoin.com adds: “In recent years, Ukraine has become a regional leader in crypto adoption and the government in Kyiv has taken steps to legalize transactions with virtual assets. Crypto mining, however, needs further regulation as it’s still a gray zone.” ([Security Service of Ukraine Shuts Down Crypto Mining Farm Near Front Line in Kharkiv – Mining Bitcoin News](#))

July 20, 2022 – The FBI is hosting representatives of five Ukrainian government agencies on a visit to the United States to meet with U.S. officials, CyberScoop reports today. The SSSCIP, Prosecutor General’s Office, the Security Service of Ukraine, the Cyber Police, and the National Cybersecurity Coordination Center are part of the delegation. They plan to meet with CISA Director Jen Easterly next week and with the State Department and other agencies during their stay. Victor Zhora of SSSCIP tells CyberScoop they are especially interested in studying U.S. methods for coordination among cybersecurity agencies. ([FBI flew cyber officials from Ukraine to U.S. for training, Ukrainian official says \(cyberscoop.com\)](#))

July 20, 2022 – USCYBERCOM issues a security alert in the form of the following tweets:

“UAUS Ukrainian partners are actively sharing malicious activity with us to bolster collective cybersecurity, as we share w/them. Thanks to close collaboration with @servicessu, we are disclosing IOCs associated w/malware recently found in Ukrainian networks.”

“We are publicly disclosing these IOCs from our Ukrainian partners @servicessu to highlight potential compromises & enable collective security. We continue to have a strong partnership in cybersecurity between our two nations.”

“The Ukrainian SBU @servicessu discovered several types of malware in their country & analyzed the samples to identify indicators of compromise – the list includes 20 novel IOCs in various formats. [More here.](#)”

([https://twitter.com/CNMF\\_CyberAlert/status/1549764857972621322](https://twitter.com/CNMF_CyberAlert/status/1549764857972621322))

Maj. Katrina Cheesman, a spokeswoman for the Cyber National Mission Force, confirms: “These indicators of compromise were shared with us by our Ukrainian partners to enable industry to take action and assess their own networks.” ([Ukraine News: Kyiv Intensifies Attacks on Russian Positions in South - The New York Times \(nytimes.com\)](#))

July 20, 2022 – The Aspen Security Summit includes numerous comments about the unexpected lack of heavy Russian use of cyberattacks in Ukraine.

*Politico’s* Shane Harris tweets: “The question has come up several times at #AspenSecurity, why didn’t Russia launch cyber attacks on US critical infrastructure in retaliation for Ukraine-related sanctions? Several theories, some of which boil down to: those attacks are hard, they take time to plan ... Russia has its hands full



fighting a war and has no interest in provoking a US response to a critical infrastructure attack, which they believe would be significant.”

(<https://twitter.com/shaneharris/status/1549794760398872577>)

In a separate article for *Politico*, Harris summarizes some of the points raised: “U.S. officials are still struggling to determine why Russia has held back on unleashing the full extent of its cyber capabilities against Ukraine and its allies, even as Moscow hasn’t entirely thrown cyber by the wayside.

“Anne Neuberger, the White House deputy national security adviser for cyber and emerging technology, noted that ‘one of the possibilities’ could be that Russia was not fully prepared to use its cyber arsenal. Neuberger said other options could be that Putin was deterred after Biden warned him of negative consequences. It’s also possible Ukraine’s effort to strengthen its critical infrastructure paid off, she said.

“‘We don’t quite know ... but certainly something we’re watching very closely,’ Neuberger told the Aspen crowd.

“Senate Intelligence Committee Chair Mark Warner (D-Va.) said he believed the world had not yet seen Russia’s ‘full cyber power,’ and he warned that Sweden and Finland’s entry into NATO could be tempting targets for future Russian cyberattacks.

“Microsoft President Brad Smith noted that while Russia may have held back, it has certainly used cyber as part of its strategy. Microsoft has seen Russia employ ‘destructive cyberattacks,’ espionage efforts and disinformation, Smith said. Microsoft released a report last month detailing such Russian operations.

“‘There is sort of a view that Russia hasn’t taken many steps in Ukraine in terms of cyber,’ said Matthew Olsen, assistant attorney general for national security at the Justice Department. ‘That is a myth, and we are effectively seeing a hot cyber war in Ukraine carried out by the Russians.’” ([Fear and loathing in Aspen - POLITICO](#); see the Neuberger video here: [Fireside Chat on Cyber, Crypto, and Quantum with Anne Neuberger - YouTube](#))

July 20, 2022 – Anne Neuberger’s opening comment at Aspen on lessons from Ukraine so far (from the YouTube video starting at the 4:32 mark):

“We learned a lot in the way the Russians really used cyber operations as part of their brutal invasion of Ukraine. At first, we’ve seen several different variants of destructive malware use. When we think about cyber operations, there are certainly cyber operations for intelligence purposes and there are cyber operations to disrupt or degrade communications systems or power systems, as part of, for example, Russia’s invasion of Ukraine, Russia’s desire to coerce that population. And we certainly saw that closely aligned with its invasion, to inform both in advance as well as to accelerate its invasion. With regard to your question about what we learned about it and working with the Ukrainians – we worked very closely with the Ukrainians for years prior to Russia’s further invasion of Ukraine – we really learned three things.

“First, the degree of preparation – the resilience of critical infrastructure, incident response planning – is key for a country. Ukraine experienced disruptive cyberattacks the last time Russia went into Ukraine in 2014 and 15, and they saw

that one of the reasons they were so susceptible was, frankly, they still had the integrated energy infrastructure from the Soviet era. So, they made a huge push to move off that integrated energy infrastructure and in fact, literally, in the weeks prior to Russia's invasion they cut that dependency and then later connected to the European grid – a really critical point about resilience of critical infrastructure.

“Similarly, incident response planning – being prepared to consider – they expected the incidents and worked closely to prepare for it [sic]. And we had teams on the ground from various agencies – virtually and on the ground – helping as well. And, truly, that lesson is what led to our announcement of building out a NATO cyber capability – a virtual cyber capability – so NATO nations could be prepared to offer incident response capabilities in the event of an attack on an ally. And I traveled three times to NATO, in October, February, and May, for the U.S. to urge that standing up of that capability.

“And then, finally, a core lesson – about the role of the private sector, the visibility of the private sector, the power of cooperation across the sector as many companies surged in to help Ukraine, and the role of information operations.”  
([Fireside Chat on Cyber, Crypto, and Quantum with Anne Neuberger - YouTube](#))

July 20, 2022 – Ukraine's first lady, Olena Zelenska, addresses the U.S. Congress, a rare event for the spouse of a foreign leader, in which she asks for more American aid for Ukraine's war efforts. ([E.U. Nations Are Asked to Ration Gas: Russia-Ukraine Live Updates - The New York Times \(nytimes.com\)](#))

July 20, 2022 – Reflecting an effort to share useful data on the cyber conflict over Ukraine with the public, USCYBERCOM posts technical data relating to various kinds of malware said to be targeting Ukrainian systems recently. The information comes from the Ukrainian government. The Command in turn shares it with a number of private sector open websites, including [VirusTotal](#), [Pastebin](#), and [GitHub](#). Posting on Pastebin, the Cyber National Mission Force says: “CNMF is disclosing these IOCs in close coordination with our Ukrainian counterparts. The Security Service of Ukraine discovered several types of malware in their country over the last few months, and have analyzed the samples and identified IOCs. The IOCs included 20 novel indicators in various formats.” ([U.S. Cyber Command exposes malware targeting Ukrainian entities \(cyberscoop.com\)](#); [Ukraine Network IOCs July 20 2022 - Pastebin.com](#))

Mandiant provides more specifics: “We are highlighting UNC1151 and suspected UNC2589 operations leveraging phishing with malicious documents leading to malware infection chains. Indicators used in these operations have been released by U.S. CYBERCOMMAND. UA CERT has also published on several of these operations.” ([Evacuation and Humanitarian Documents used to Spear Phish Ukrainian Entities | Mandiant](#))

July 20, 2022 – Reuters publishes an elaborate, graphics-laden takeout on the evolution of the Ukraine war, relying on satellite mapping data from the private Australian Strategic Policy Institute and other commercial satellite imagery. While not directly cyber-related, Reuters' dramatic portrayal demonstrates another way in which high

tech advances and access to data (often from private sector sources) can have impact – in this case, on improving the public’s ability to learn about and understand the conflict. ([The Road to Stalemate in the Russia-Ukraine War \(reuters.com\)](#))

July 21, 2022 – Ukrainian company TAVR Media reports a cyberattack aimed at spreading a false message that President Zelensky is in intensive care and that the head of the Verkhovna Rada has taken charge. Zelensky posts on Instagram that he has “never felt as strong as I am now.” There is no official word on the perpetrator, though Zelensky blames Russia. ([Cyber criminals attack Ukrainian radio network, broadcast fake message about Zelensky's health \(cyberscoop.com\)](#))

July 21, 2022 – Computer security firm Akamai reports it has “detected and mitigated the largest DDoS attack ever launched against a European customer on the Prolexic platform, with globally distributed attack traffic peaking at 853.7 Gbps and 659.6 Mpps over 14 hours. The attack, which targeted a swath of customer IP addresses, formed the largest global horizontal attack ever mitigated on the Prolexic platform. The victim, an Akamai customer in Eastern Europe, was targeted 75 times in the past 30 days with horizontal attacks.” ([Largest European DDoS Attack on Record | Akamai](#))

July 22, 2022 – The head of the self-proclaimed Donetsk People's Republic (DPR), Denis Pushilin, posts on Telegram that the separatist region has blocked access to Google because of its alleged promotion of “violence against all Russians” with backing from its “handlers from the U.S. government.” ([Russian-backed separatists in Ukraine block Google search engine | Reuters](#))

July 22, 2022 – The head of Latvia’s Cert.lv, the Information Technology Security Incident Response Institution, reports that the country is facing around 1,000 cyberattacks per day, the most worrisome being against private firms providing services to the state and critical infrastructure. Baiba Kaskina says the situation “has never before been so tense.” She suggests the more serious attacks on critical infrastructure are connected to Russian intelligence agencies but that the number of “commercially motivated” hits has also risen after a temporary dip following the start of the Ukraine war. Cert.lv is attached to the University of Latvia's Institute of Mathematics and Computer Science and is responsible to the Ministry of Defense. ([Situation in Latvia's cyberspace has never before been so tense - Cert.lv \(baltictimes.com\)](#))

A later report ties a 12-hour attack on Latvia’s public broadcasting center around this time to the pro-Russia hacker group Killnet, noting that it followed the government’s announcement it had destroyed almost 300 Soviet monuments. ([Pro-Kremlin hackers target Latvia’s parliament after declaring Russia a sponsor of terrorism - The Record by Recorded Future](#))

July 22, 2022 – Reflecting another element of U.S. cyber activity relating to the Ukraine war, Lt. Gen. Kevin Kennedy, the new head of Sixteenth Air Force (Air Forces Cyber), tells reporters his group will continue with existing plans to ensure readiness on the part of the U.S. European Command in its role as the service’s component to Cyber

Command. Kennedy's group provides personnel and conducts a variety of cyber, electronic warfare, and intelligence operations, according to a media report. ([Air Force cyber chief sees enduring support in Europe as war rages on - The Record by Recorded Future](#))

July 22, 2022 – A podcast interview spotlights one effort to help Ukraine defend its critical infrastructure – cyberwar.com.ua. The joint campaign involves two private groups – Hideez Group Inc. (a U.S.-Ukrainian enterprise identity startup based in Kyiv) and Yubico (“A world leading manufacturer of multifactor authentication solutions” that earned a “best security key” from ZDNet)) – focusing on FIDO solutions. Their goal is to obtain and distribute 100,000 security keys by the end of 2022 and 1 million by the end of 2023. So far they have received 30,000 keys for distribution. The effort is cooperating with the Ministry of Digital Transformation, the State Service of Special Communications and Information Protection of Ukraine as well the “largest critical infrastructure providers.”

In their appeal for donations of all kinds of computer hardware, they underscore Ukraine's remarkable success: “[A] quarter of Ukraine is destroy[ed], and yet, anyone with internet can order new passport, open a bank account, sell and buy properties, pay taxes. Ukraine's digital initiatives, and upfront work to create strong digital networks, now pays off. Digitalization is the new national security foundation.” They further define the problem as global: “Helping us defending Ukraine, means that you don't have to worry about defending your own country from the same crisis. This war is not about Ukraine vs Russia. This is Putin vs all civilised world. Ukraine must win.” ([Cyberwar.com.ua](#))

July 22, 2022 – A report by C4ISRNET assesses Russia's surprisingly limited efforts to jam GPS in Ukraine. (However, see also April 11, 2022, entry above.) The report notes that Russian forces have regularly jammed such targets because of their critical importance to modern warfare, yet they have not been nearly as aggressive as many expected. Experts see a number of possible reasons, including: Russia's capabilities are not as good as expected; Russian forces themselves depend on GPS; high-powered jammers are easy to block; Ukraine is still using a huge amount of Soviet-era weaponry that predates GPS and even other kinds of electronic warfare; Putin may be waiting to use his most potent electronic weapons against U.S. and NATO forces, if it comes to a direct conflict. ([Why isn't Russia doing more to jam GPS in Ukraine? \(c4isrnet.com\)](#))

July 22, 2022 – DISA grants a six-month extension on Booz Allen Hamilton's contract (see January 24, 2022, entry) to produce a zero trust Thunderdome Prototype so that it can include the military's classified SIPRNet network. DISA says the need to upgrade the “antiquated” Secure Internet Protocol Router Network is one of the lessons gleaned from the war in Ukraine. ([News \(disa.mil\)](#))

July 25, 2022 – A report in the Financial Times describes wide-ranging efforts by tech executives and other expat Ukrainian professionals to help their country in what Andrey Liscovich and Oleg Rogynskyy, two “tech-savvy executives,” call “the world's



first open-source war.” Activities include locating experts, disseminating supplies, and fund-raising. Their experience and “broad digital connections in various fields” have created “lateral networks” drawing on “a homegrown ecosystem of IT talent.” ([Financial Times](#); *The Cipher Brief*, 7-25-22)

July 26, 2022 – Former Estonia President (2006–2016) Toomas Hendrik Ilves calls for a “digital alliance” among democratic states “that is really and truly value[s]-based ... and is not bound by geography.” Addressing a virtual security forum hosted in Taipei, Ilves points out that almost every sector from industry to politics relies on digital platforms, which has produced new security threats. That in turn has morphed the nature of modern warfare. ([Estonia ex-leader calls for 'digital alliance' to combat cyber threats - Focus Taiwan](#))

July 26, 2022 – Cloudflare tweets: “Complete #Internet outage in #Kherson, #Ukraine between 0640-1115 UTC today follows an observed disruption starting at 1910 UTC on Sunday. Sunday's disruption was driven by outages across multiple networks including AS56404, AS47598, and AS56446.” ([Twitter](#))

July 27, 2022 – Europe’s second highest court rebuffs Russia Today’s legal challenge to the EU’s ban on RT broadcasting in Europe. “The Grand Chamber of the General Court dismisses RT France's application for annulment of acts of the Council, adopted following the outbreak of the war in Ukraine, temporarily prohibiting that organisation from broadcasting content,” the Luxembourg-based court said in a statement. ([Russia Today loses fight against EU ban, Moscow warns of retaliation | Reuters](#))

July 27, 2022 – CISA and Ukraine SSSCIP sign a Memorandum of Cooperation to expand their ongoing cybersecurity relationship. Specific areas of collaboration include:

- Information exchanges and sharing of best practices on cyber incidents;
- Critical infrastructure security technical exchanges; and
- Cybersecurity training and joint exercises.

(Text of MOC, 7-27-22)

July 27, 2022 – *The Record* posts an article about the group DDoSecrets and its emergence as the “go-to home for Russian leaks.” The group’s website has posted 58 Russian data dumps with more than 12 million documents since Russia’s invasion of Ukraine. Among the more active leakers are Anonymous, Ukrainian Cyber Alliance, and CyberHunta. DDoSecrets has also received leaks of Ukrainian data but to date has not posted any of them because “they’ve all been identified as likely tied to state-sponsored entities or as active parts of psyops,” or lack a clear justification for publishing in the public interest, according to co-founder Emma Best. ([How DDoSecrets built the go-to home for Russian leaks - The Record from Recorded Future News](#))

Late July 2022 – CyberCube, a risk analytics firm specializing in the cyber insurance market, publishes a “Global Threat Briefing” for the second half of 2022, which

notes: “There are currently more than 70 different cyber threat actors related to the war in Ukraine – double the number identified at the beginning of March. Russia is targeting governments outside of Ukraine in cyber espionage campaigns to gather intelligence on Western initiatives to assist Ukraine’s war effort. Since the start of the war, Microsoft has detected Russian network intrusion attempts against 128 targets in 42 countries outside of Ukraine. Russia is still heavily focussed on merging its military efforts with cyber operations inside Ukraine, including staging targeted attacks on communications and logistics systems and nuclear power facilities. Microsoft noted Russia’s more recent destructive cyber attacks have been coordinated with missile attacks and have targeted Ukraine’s railways and transportation systems used to move weapons and military supplies.” ([\(Report\) CyberCube Global Threat Briefing H2 2022.pdf \(cybcube.com\)](#))

Late July 2022 – Hackers publish over 10 million data points about past shipments reportedly stolen from the official Russian Postal Service, including sender and recipient names, addresses, and other details. Pochta denies it was breached, saying the theft was from a third-party contractor. Previous data leaks from Russian delivery services have come from Yandex Food, DeliveryClub, and CDEK. ([RiskBiz News: Confluence servers under attack due to hardcoded password \(substack.com\)](#))

Late July 2022 – APT group Gamaredon ramps up the frequency of its attacks and number of bait deliveries targeting military and police entities in Ukraine's Kherson Oblast, Donetsk Oblast and other regions, cybersecurity firm NSFOCUS reports. The Russian group first appeared in 2013 and has long focused on Ukrainian and other East European government departments. “Combined with Gamaredon's previous attacks and current developments, we speculate that the second peak of attacks in late July may mark the arrival of a new Russian action,” NSFOCUS concludes. ([In a three-pronged approach, APT group Gamaredon has recently stepped up its cyber offensive against Ukraine – the NSFOCUS TechNolog](#))

July 27, 2022 – Senator Bob Menendez (D-NJ), chair of the Senate Foreign Relations Committee, Senator Tim Kaine (D-VA), and Senator Bill Cassidy (R-LA) send letters to Meta, Facebook, Twitter, and Telegram asking them to do more to block Spanish-language disinformation on Ukraine from Russian sources including RT en Espanol and Sputnik Mundo. This follows a similar letter to Facebook in April from 21 lawmakers. ([Bipartisan U.S. lawmakers urge Facebook, Twitter to better fight Russian disinformation | Reuters](#))

July 28, 2022 – Moscow's Tagansky District Court orders WhatsApp to pay a fine of 18 million rubles (\$301,255). The court also fines Tinder owner Match Group 2 million rubles, Snap and Hotels.com 1 million rubles, and Spotify 500,000 rubles. The offense, according to Roskomnadzor, is failure to document that they are storing and processing Russian user data. ([Russia fines WhatsApp, Snap and others for storing user data abroad | Reuters](#))

July 29, 2022 – Website Planet publishes a lengthy article titled: “Is Anonymous Rewriting the Rules of Cyberwarfare?” Security researcher Jeremiah Fowler details how the group, founded in 2003 and known before the Ukraine war as “little more than cyber vandals” and pranksters, has become an extraordinarily effective disruptor of Russian computer networks and official activities. Among the methods Fowler calls new and hard to defend are: hacking printers to print pro-Ukrainian messages (including on grocery store receipts); using Conti’s ransomware code to encrypt Russian data; hijacking servers to get past geofencing and conduct disruptive operations; hacking TV news programming; targeting companies doing business with Russia; bypassing censors by using robocall and SMS technology to send over 100 million messages about the war to Russian devices; and leaking stolen data online. “The group has demystified Russia’s cyber capabilities and successfully embarrassed Russian companies, government agencies, energy companies and others,” Fowler told *Express*. ([Is Anonymous Rewriting the Rules of Cyberwarfare? Timeline of Their Attacks Against the Russian Government \(websiteplanet.com\)](#); [Is Anonymous Rewriting the Rules of Cyberwarfare? Timeline of Their Attacks Against the Russian Government \(websiteplanet.com\)](#))

July 29, 2022 – KillMilk, leader of the Kremlin-linked hacktivist group Killnet, announces that he will soon be leaving the group to form another entity – after he mounts a hack and leak operation against defense contractor Lockheed Martin, maker of the HIMARS missile. On August 1, Sputnik quotes KillMilk as declaring, “starting today, defense industry corporation Lockheed Martin will be a target of my cyberattacks. I am against weapons. I am against merchants of death.” The new head of Killnet will reportedly be a person with the cover name “BlackSide.” ([KillNet threatens hack-and-leak op against HIMARS maker. Online investment scams hit Europe. Microsoft associates Raspberry Robin with EvilCorp. \(thecyberwire.com\)](#))

July 30, 2022 – A lengthy article in IEEE Spectrum analyzes Russia’s surprisingly ineffective use of electronic warfare (EW) in Ukraine. “[I]n the early days of the 24 February invasion, analysts expected Russian forces to quickly gain control of, and then dominate, the electromagnetic spectrum. Since the annexation of Crimea in 2014, EW has been a key part of Russian operations in the ‘gray zone,’ the shadowy realm between peace and war, in the Donbas region. Using Leer-3 EW vehicles and Orlan-10 drones, Moscow-backed separatists and mercenaries would jam Ukrainian communications and send propaganda over local mobile-phone networks. When Russian forces were ready to strike, the ground and airborne systems would detect Ukrainian radios and target them with rocket attacks. But after nearly a decade of rehearsals in eastern Ukraine, when the latest escalation and invasion began in February, Russian EW was a no-show.” ([The Fall and Rise of Russian Electronic Warfare \(ieee.org\)](#))

Summer 2022 – British authorities discover that Liz Truss’ mobile phone was hacked while she was foreign minister, according to the *Daily Mail*. Unnamed sources in the report say Russian spies are suspected. Then-Prime Minister Boris Johnson reportedly ordered the event be kept quiet. *Seriously Risky Business* later provides some caveats

on the story – including a link to a separate analysis of it, which concludes that it “could be true.” ([Truss phone hacked by Putin spies for top secret information - The Mail \(mailplus.co.uk\)](#); [UK politicians demand probe into Liz Truss phone hack claim | AP News](#); Risky Biz News, 11-2-2022)

August 2022 – Russian forces in Kherson release a Ukrainian resistance fighter named Ihor after 11 days of detention and torture. But their objective in doing so is to use him to seize other dissidents, in part by tracking his Telegram communications with a Ukrainian special forces officer named “Smoke.” How they went about this – and the flaws in Telegram’s security the episode reportedly exposes – are the subject of a later, sharply critical analysis in the outlet *PwnAllTheThings*. ([Russia is spying on Telegram chats in occupied Ukrainian regions. Here's how. \(pwnallthethings.com\)](#); [Stealthy Kherson resistance fighters undermined Russian occupying forces - The Washington Post](#))

August 1, 2022 – Killnet targets Lockheed Martin, claiming to steal employee data, according to the *Moscow Times* and *Newsweek*. The company does not initially make a public statement. ([Killnet Releases 'Proof' of Its Attack Against Lockheed Martin | SecurityWeek.Com](#))

August 3, 2022 – Nathaniel Fick, nominee to be the State Department’s first Ambassador-at-Large for Cyberspace and Digital Policy, tells Senators at his confirmation hearings that in terms of policy challenges, “The wolf closest to the door, so to speak, in my view is the Russian invasion of Ukraine, and the threats and opportunities it provides in the digital space for us.” He adds, “And then I believe our strategic competition with China, along digital lines, is probably the defining strategic question of my generation.” ([Cyber Ambassador Pick Wants to Bring 'Coherence' to Tech Diplomacy Efforts - Defense One](#))

Early August 2022 – Nozomi Networks Labs releases a 2022 1H Review that concludes: “It is clear that cyberattacks have become a force multiplier during conflict ... Here is what we can learn from this war: War increases cyber activity: Of the varying threat actors and motives, nation-state Advanced Persistent Threats (APTs) are the most active during wartime. They are less financially motivated and more focused on cyber espionage—spying and disrupting communications and other critical enemy systems. Some companies become incidental casualties of cyber war as a result of threat actors’ attacks on their targets.” ([Nozomi-Networks-OT-IoT-Security-Report-2022-1H.pdf \(nozominetworks.com\)](#))

August 4, 2022 – Ukraine’s Security Service reports it has taken down a botnet operation comprising 1 million bots that had been using fictitious accounts to spread false information about alleged conflicts between the President’s Office and the head of the armed forces and even targeted President Zelensky’s wife. The SSU identifies the head of the hacker group as a “Russian citizen who has lived in Kyiv and positioned himself as a ‘political expert.’” (<https://the cyberwire.us16.list->



[manage.com/track/click?u=9f0cab23b3ee44f3bc482be80&id=39f11f3ec5&e=bfa0e2e30b](https://manage.com/track/click?u=9f0cab23b3ee44f3bc482be80&id=39f11f3ec5&e=bfa0e2e30b))

August 4, 2022 – Meta’s Second Quarter 2022 Adversarial Threat Report describes the company’s threat research into a troll farm in St. Petersburg, Russia, which “unsuccessfully attempted to create a perception of grassroots online support for Russia’s invasion of Ukraine by using fake accounts to post pro-Russia comments on content posted by influencers and media on Instagram, Facebook, TikTok, Twitter, YouTube, LinkedIn, VKontakte and Odnoklassniki.” Meta identifies the perpetrators as the “self-proclaimed entity CyberFront Z and individuals associated with past activity by the Internet Research Agency (IRA).” Olga Belogolova of Meta tweets that the company has labeled the group “‘the Z Team’ largely because of how clumsy and ineffective they were.” ([Meta’s Adversarial Threat Report, Second Quarter 2022 | Meta \(fb.com\)](#); [Global network of fake news sites push Chinese propaganda, researchers find | The US made a breakthrough battery discovery- then gave the technology to China | Meta has banned a pro-Russia troll group \(substack.com\)](#))

August 8, 2022 – Reuters publishes a lengthy special report showing that Western computer components are still finding their way into Russian hands and being used in the war in Ukraine, despite sanctions and the stated intent of tech companies to stop exports to Russia. “While some of the more sophisticated Western chips in the Russian weapons have been subject to special export licensing requirements for years, the investigation found that many of the armaments also contain run-of-the-mill computer chips and other components found in consumer products. These are easily obtainable and in many cases aren’t subject to export restrictions,” the article states. Reuters found that thousands of shipments were made by third-party sellers. Among the companies whose components are still being found in Russian munitions are: Texas Instruments, Inc.; Altera, owned by Intel Corp; Xilinx, owned by Advanced Micro Devices Inc (AMD); Maxim Integrated Products Inc, acquired recently by Analog Devices Inc.; and Cypress Semiconductor, now a part of Infineon AG (Germany). ([As Russian missiles struck Ukraine, Western tech still flowed \(reuters.com\)](#))

August 9, 2022 – Russia launches an Iranian satellite, “Khayyam,” described by Iran as the start of “strategic” aerospace cooperation with Moscow. The *Washington Post* cites two sources saying the Kremlin plans to use the satellite for several months to surveil Ukrainian military targets, but the Iranian Space Agency denies this. ([Iran’s ‘Khayyam’ satellite blasts off from Moscow-operated Baikonur Cosmodrome | The Iran Project](#); [Russia to launch spy satellite for Iran but use it first over Ukraine - The Washington Post](#))

August 9, 2022 – A *New York Times* article reports on “how Russia took over Ukraine’s internet in occupied territories.” Citing the experience in Kherson as representative, the piece cites Ukrainian sources recounting occupying troops systematically forcing local Ukrainian internet service providers to relinquish control of their networks (they “put guns to their head[s],” said one source), then rerouted data

through Russian networks, blocking access to Western social media in the process. “To cap off that control, Russia has also begun occupying the cyberspace of parts of those areas,” the article continues. “That has cleaved off Ukrainians in Russia-occupied Kherson, Melitopol and Mariupol from the rest of the country, limiting access to news about the war and communication with loved ones. In some territories, the internet and cellular networks have been shut down altogether. Restricting internet access is part of a Russian authoritarian playbook that is likely to be replicated further if they take more Ukrainian territory,” the article postulates. ([How Russia Took Over Ukraine’s Internet in Occupied Territories - The New York Times \(nytimes.com\)](https://www.nytimes.com/2022/08/09/technology/russia-ukraine-internet-occupied-territories.html))

August 9, 2022 – The pro-Russia hacker group NoName057(16) takes down the Finnish parliament’s website from about 2:30 p.m. to 10:00 p.m. “We decided to make a ‘friendly’ visit to neighbouring Finland, whose authorities are so eager to join Nato,” the group says on its Telegram channel. Finland’s National Cyber Security Centre reports the attack originated from dozens of IP addresses around the world, according to Yle News. ([NBI launches probe into attack on Finnish Parliament site | News | Yle Uutiset](https://yle.fi/en/news/finland-launches-probe-into-attack-on-finnish-parliament-site))

August 9, 2022 – The U.K.’s National Cyber Security Center (NCSC) and Scotland Yard are investigating several DDoS attacks against cryptocurrency exchange firm Currency.com that it suspects are of Russian origin. In late February, Victor Prokopenya, founder of VP Capital which owns the company, criticized the Ukraine war. He tells *The Telegraph*: “The cyber attack has been going on almost on a daily basis every day for the last three months. It’s like someone repeatedly trying to break down your front door.” NCSC reportedly believes the perpetrators are private actors rather than Russian government entities. ([Suspected Russian cyber attack on British soil as firm subjected to ‘daily’ hacks \(telegraph.co.uk\)](https://www.telegraph.co.uk/technology/2022/08/09/suspected-russian-cyber-attack-on-british-soil-as-firm-subjected-to-daily-hacks/); The CyberWire, 8-13-22)

August 10, 2022 – The *Washington Post* reports on Russia’s ability to maintain a wide-ranging social media presence by exploiting loopholes in the rules of platforms like Facebook, YouTube, and Twitter. “Russian Embassy accounts in countries around the world have actually received more engagement on Facebook and Twitter since the war began” than before the February 24 invasion, the Post reports, citing a report from a research group, Advance Democracy, Inc. (The report is not cited directly here because the editors of this timeline could not locate it anywhere on the web, including on ADI’s own website.) “On Facebook, those accounts have found ways to launder Russian propaganda from sanctioned state media accounts, such as copying and embedding videos originally produced by state-run Russia Today rather than linking to them.” George Dubinskiy, Ukraine’s deputy minister of digital transformation, comments that Russia is very familiar with the “vulnerabilities” of various internet platforms, adding: “We have a media war right now.” ([Big Tech effort to quash Russian propaganda about Ukraine failed - The Washington Post](https://www.washingtonpost.com/technology/2022/08/10/russia-social-media-ukraine-war/))

August 10, 2022 – The “Elves,” a growing collective of “ordinary citizens from across Central and Eastern Europe” with cyber expertise receives media coverage in CyberScoop for their increasingly effective campaign to counter Russian disinformation in and around Ukraine. The group formed in 2014 in Lithuania but has since expanded to several thousand volunteers. (See the GMF paper cited in a January 2022 article, above.) One of the movement’s founders explains the name: “Trolls are ugly; elves are bright creatures confronting them ... fighting against evil.” ([Collective of anti-disinformation 'Elves' offer a bulwark against Russian propaganda \(cyberscoop.com\)](#))

August 10-11, 2022 – Viktor Zhora, deputy head of Ukraine’s State Service of Special Communications and Information Protection, speaks publicly about the situation in Ukraine during a visit to Las Vegas for the Black Hat convention. He says that cyber incidents against Ukraine have tripled since late February, calling it “perhaps the biggest challenge since World War II for the world, and it continues to be completely new in cyberspace.” In an interview the day before, however, he assesses Russia’s overall approach to conducting cyberattacks as “chaotic” and indicating an “absence of strategy” or coordination. Most of the attacks, he notes, are DDoS hits, defacements, vulnerability exploits, data exfiltration attempts, or involve interference with media. Skill levels of the perpetrators vary. CyberScoop notes two “notable exceptions”: the Viasat hit on February 23-24 and the strike against the country’s electrical grid on April 8 (see entries above).

In a separate interview with Reuters, Zhora comments that Microsoft, Amazon, and Google have helped move Ukrainian government data to “multiple countries” in Europe. ([Ukraine cyber chief pays surprise visit to 'Black Hat' hacker meeting in Las Vegas | Reuters; Russia's digital attacks are haphazard, chaotic, says top Ukrainian cyber official - CyberScoop](#))

At some point during his Las Vegas visit, Zhora accuses Russia of committing cyber “war crimes.” “Since most [Russian] kinetic operations focused on civilian infrastructure and cyber operations supportive of that are exactly the same type of thing, hitting civilian IT infrastructure,” Zhora tells *Motherboard*. “These cases we can treat them as war crimes in cyberspace.” ([Head of Ukraine’s Cybersecurity Says Russia Has Committed ‘Cyber War Crimes’ \(vice.com\)](#))

Zhora’s comments meet with skepticism and even concern in some circles. The news analysis service *Seriously Risky Business* posts a comment on August 17 (see entry below) questioning whether Zhora’s statements and public pronouncements by others may be exaggerating the situation. ([When Sanctioning Code Makes Sense - by Tom Uren \(substack.com\)](#))

August 11, 2022 – Latvia’s parliament reports it has been hit by a DDoS attack. “The Saeima has adopted a statement in which Russia is recognized as a country that supports terrorism. There is a large-scale DDoS attack against the Saeima’s resources by activists supporting RU aggression. Thanks to @mans\_tet and previously prepared defense solutions, the work of the Saeima has not been disturbed.” Killnet claims responsibility. ([Twitter](#);

<https://mail.google.com/mail/u/0/#inbox/WhctKKXgkHXZRlXTSsgkcTqDfSLcGRBKrVVXgNjDLHcwPcfQgbJRLQzfQLgkQlrdfMxSSLg>

August 11, 2022 – USCYBERCOM issues a Cyber National Mission Force cyber alert that reads: @RFJ\_USA [Rewards for Justice] is seeking info on individuals linked to #Conti aka Wizard Spider, a Russian government-linked ransomware group that has targeted US/Western CIKR. Offer is up to \$10 million for info leading to the identity or location of these actors.” Rewards for Justice is an interagency rewards program and CIKR stands for “critical infrastructure and key resources.” ([Twitter](#); [Conti – Rewards For Justice](#))

August 15, 2022 – A Microsoft report describes a suspected Russian hacking group that has targeted NATO member-state government organizations, think tanks, and defense contractors since at least 2017, *The Record* reports. Microsoft’s Threat Intelligence Center (MSTIC) says it has worked to disrupt activities by the group, SEABORGIUM (Callisto, COLDRIVER, TA446). ([https://therecord.media/microsoft-disrupts-russia-linked-hacking-group-targeting-defense-and-intelligence-orgs/?utm\\_source=substack&utm\\_medium=email](https://therecord.media/microsoft-disrupts-russia-linked-hacking-group-targeting-defense-and-intelligence-orgs/?utm_source=substack&utm_medium=email)Microsoft disrupts Russia-linked hacking group targeting defense and intelligence orgs - The Record by Recorded Future)

August 2022 – Sometime this month, the Russia-linked Gamaredon APT is observed to be attacking Ukrainian users with malware that steals information through use of phishing documents with lures relating to the Ukraine war. Cisco’s Talos Group reports this finding in mid-September. ([Gamaredon APT targets Ukrainian government agencies in new campaign \(talosintelligence.com\)](#))

August 2022 – Starting this month, according to computer intelligence firm Recorded Future, the threat activity group UAC-0113 (as tracked by CERT-UA) has been steadily expanding its activities in Ukraine by disguising itself as various Ukrainian telecommunication providers and using spearphishing campaigns or redirects that threaten targeted networks. The company links UAC-0113 to Sandworm with “medium confidence.” ([Message from Recorded Future; Russia-Nexus UAC-0113 Emulating Telecommunication Providers in Ukraine \(recordedfuture.com\)](#))

Mid-August 2022 – Dell closes its offices in Russia. The company is reportedly a vital supplier of servers. (ASPI, Daily Cyber Digest, 8-29-22)

August 16, 2022 – An Axios Codebook piece describing the Biden White House’s “three-headed cybersecurity team” of Chris Inglis, Jen Easterly, and Anne Neuberger notes a degree of confusion for outsiders over who does what, but inserts the comment that the war in Ukraine has “left little room for turf wars.” ([Biden's 3 cyber heads \(axios.com\)](#))

August 16, 2022 – Reuters reports that a Russian court has fined the U.S.-based streaming service Twitch 2 million rubles (\$33,000) for hosting a video with “fake”



information alleging war crimes in Bucha, Ukraine. ([Russia fines streaming site Twitch over 31-second 'fake' video, Russian media report | Reuters](#))

August 16, 2022 – Ukraine’s state corporation Energoatom tweets: “⚠️ Rashists have launched an unprecedented cyberattack on the official website of Energoatom. Today, August 16, 2022, the most powerful since the beginning of the full-scale invasion of the Russian Federation hacking attack on the official website of DP “NAEK” [“Energy”] took place. [It] was attacked from the territory of the Russian Federation. The Russian group “narodnaya kiberarmiya” launched a cyberattack using 7.25 million bot users who simulated hundreds of million views of the company’s homepage for three hours. The mentioned attack did not significantly affect the work of the site of the DP “NAEK” [“Energoatom”] and remained nominal 3a [sic] users.” ([Twitter](#))

The *New York Times* notes that, while it failed, the attack is a “reminder of the digital threat posed to the power infrastructure in Ukraine, where the shelling of the Zaporizhzhia Nuclear Power Plant has stirred global alarm.” ([The operator of Ukraine’s nuclear plants says it faced an ambitious cyberattack. - The New York Times \(nytimes.com\)](#))

August 16, 2022 – Lt. Gen. Maria Gervais, deputy commanding general and chief of staff at Training and Doctrine Command (TRADOC), discusses some lessons the U.S. Army has learned in the Ukraine war at the TechNet Augusta (Ga.) conference. “If we’re looking to see how a modern battlefield is impacted by EW and cyber warfare, we need to look no further than what is going on right now” in Eastern Europe, Gervais says. “Everything that we are seeing in Ukraine has implications for a unified network, and almost certainly represents the type of threats we will see.”

One conclusion Gervais and others have drawn is that cyber and electronic warfare need to be combined with other weapons to be fully effective in battle. “Neither [cyber nor EW] is dominant on its own and they work best when converged with other multi-domain effects,” Gervais says. In “gray zone” competition, non-kinetic tools are relatively more effective.

Gavin Wilde of the Carnegie Endowment for International Peace and a former NSC staffer tells Fedscoop that Russian use of cyber and EW don’t appear to have provided the capability to make big gains on the battlefield. But EW seems to have enhanced their artillery advantage. Still: “There have been far fewer, if any, examples of ‘lessons learned’ or any kind of ‘re-emergence’ of cyber capabilities in support of kinetic action since late February.” ([Army lesson from Ukraine war: cyber, EW capabilities not decisive on their own \(fedscoop.com\); Ukraine ‘testing ground’ shaping US network, electronic warfare effort \(c4isrnet.com\)](#))

August 17, 2022 – The news analysis service *Seriously Risky Business* posts a comment that raises the question whether statements by Ukrainian cybersecurity official Victor Zhora and others, including Microsoft, may be overstating the true state of affairs involving cyber in Ukraine. Under the header “Cyber War Crimes are Not a Thing,” Tom Uren writes: “Some of Zhora’s comments reinforced concerns this newsletter

has held that the importance or impact of Russian cyber operations in Ukraine are being exaggerated.” Uren continues: “There may well be Russian cyber operations that are war crimes, or contributed to war crimes, and they absolutely should be prosecuted. But we don't think that talking about them in isolation as ‘cyber war crimes’ is useful — cyber operations are just a standard part of warfare nowadays and we wouldn't talk about ‘air force war crimes’ or ‘navy war crimes’.” ([When Sanctioning Code Makes Sense - by Tom Uren \(substack.com\)](#))

August 17, 2022 – Cybersecurity firm Fortinet releases a report indicating that wiper malware has begun surfacing at an unprecedented rate, extending well beyond the Ukraine conflict to as many as 24 countries. Recorded Future's Insikt Group previously identified nine wipers in Ukraine, including WhisperKill, WhisperGate, HermeticWiper, IsaacWiper, CaddyWiper, and DoubleZero. But recently the trend has become a “truly global phenomenon,” reports *The Record*. According to a Fortinet researcher, “We saw significant spillover from attacks against Ukraine. In many cases the main target was probably a Ukrainian organization, but due to the interconnectedness of the world, these attacks can easily affect other countries.” Fortinet calls the trend “disturbing.” ([Fortinet: Use of wipers expanding beyond Ukraine to 24 countries - The Record by Recorded Future](#))

August 16-17, 2022 – Estonia faces “the most extensive cyber attacks it has faced since 2007,” according to a tweet the next day by Luukas Ilves, undersecretary for digital transformation at Estonia's Ministry of Economic Affairs and Communications. “With some brief and minor exceptions, websites remained fully available throughout the day. The attack has gone largely unnoticed in Estonia.” Killnet claims responsibility, saying it was responding to the moving of a Soviet Tu-34 tank from its location in the town of Narva to a museum. The mention of 2007 is a reference to a major attack on Estonia, which followed the removal of Soviet-era war memorials from public view. ([Estonia says it repelled major cyber attack after removing Soviet monuments | Reuters](#); [Estonia's Battle Against a Deluge of DDoS Attacks - Infosecurity Magazine \(infosecurity-magazine.com\)](#))

August 18, 2022 – Finnish firm ICEYE, which describes itself as “the global leader in persistent monitoring with radar satellite imaging,” announces it has signed a contract with the Serhiy Prytula Charity Foundation to provide Ukraine with the company's Synthetic Aperture Radar (SAR) satellite imaging capabilities. “As part of the agreement, ICEYE will transfer full capabilities of one of its SAR satellites already in orbit for the Government of Ukraine's use over the region. The SAR satellite will be operated by ICEYE. In addition, ICEYE will provide access to its constellation of SAR satellites, allowing the Ukrainian Armed Forces to receive radar satellite imagery on critical locations with a high revisit frequency.” ([ICEYE Signs Contract to Provide Government of Ukraine with Access to Its SAR Satellite Constellation](#))

August 2022 – A Ukrainian charity reportedly buys a satellite for the army after raising \$17 million for the purchase, according to *The Record*. ([Ukraine's largest charity wants to raise \\$1.3 million for 'cyber offensive' \(therecord.media\)](#))

August 18, 2022 – Trustwave posts a lengthy summary of the use of cyber weapons in the Ukraine war. The article begins: “Observing the ongoing conflict between Russia and Ukraine, we can clearly see that cyberattacks leveraging malware are an important part of modern hybrid war strategy.” The report says there is “no doubt of Russia’s involvement in the current attacks.” It lists several threat groups such as APT29 (Cozy Bear) and Sandworm along with the security agencies they are believed to be affiliated with. ([Overview of the Cyber Weapons Used in the Ukraine - Russia War | Trustwave](#))

August 18, 2022 – Trustwave further reports its finding that Russian cyberattacks against Ukraine are the work of Russian intelligence agencies not private hackers. ([Russian cyber attacks on Ukraine driven by government groups \(techtarget.com\)](#))

August 19, 2022 – GCHQ head Jeremy Fleming writes an op-ed in *The Economist*, which opens with the statement: “It is a fallacy to say that cyber has not been a factor in the war in Ukraine. Both sides are using cyber capabilities to pursue their aims. Both sides understand the potential of integrating cyber and information confrontation with their military effort. And both sides know that they are engaged in a struggle for influence and opinion far beyond the immediate battlefield. It is a very modern digital and cyber war, as much as it is a brutal and destructive physical one.”

He adds that Russia “is losing the information war, that its early planning has “fallen short,” and that its use of offensive cyber tools has been “irresponsible and indiscriminate.” But while “that’s cause for celebration, we should not underestimate how Russian disinformation is playing out elsewhere in the world.”

Fleming discloses that Russia has used similar tactics in Syria and the Balkans but that (presumably referring to the Ukraine case) GCHQ has managed to intercept Russia’s plans and warn potential targets in advance. He specifically mentions deployment of the U.K.’s National Cyber Force, a partnership between GCHQ and the Ministry of Defence, that uses offensive cyber tools. He makes a point of stating that “This secret and important work is conducted in accordance with international law and domestic legislation. It is authorised by ministers and scrutinised by judicial commissioners. It is this ethical, proportionate and legal approach that sets us apart from our adversaries and from Russia’s use of cyber capabilities in this war.” ([The head of GCHQ says Vladimir Putin is losing the information war in Ukraine | The Economist](#); [UK spy chief says Putin is losing information war in Ukraine -The Economist | Reuters](#); The Cyberwire, 8-19-22)

August 19, 2022 – Iran begins transporting Mohajer-6, Shahed-129, and Shahed-191 drones to Russia for use against Ukraine, according to U.S. officials. Each drone model is capable of carrying munitions, intelligence indicates. However technical problems have been reported, including testing failures. Experts say Iran has never tested these UAVs against the kind of sophisticated counter-systems used in

Ukraine. ([Iran sends first shipment of drones to Russia for use in Ukraine - The Washington Post](#))

August 20, 2022 – Pro-Ukrainian hackers cut into Russian TV networks in Crimea and broadcast a speech by President Zelenskyy, according to Ukrainian authorities. ([Ukrainian hackers hack Crimean TV – StratCom of the Armed Forces of Ukraine | Ukrainska Pravda](#))

August 20, 2022 – DESFA, Greece’s national natural gas operator, posts: “DESFA suffered a cyberattack on part of its IT infrastructure by cybercriminals that have tried to gain illegal access to electronic data .... We have managed to ensure and continue the operation of the National Natural Gas System (NNGS) in a safe and reliable way .... DESFA remains firm in its position not to negotiate with cybercriminals.” The CyberWire notes that “An attack on a European natural gas distributor during Russia’s war against Ukraine is consistent with privateering aligned with Moscow’s interests.” ([Announcement - desfa.gr](#); The CyberWire, Week that Was,” 8-27-22)

August 22, 2022 – Ukraine and Poland sign a memorandum of cooperation aimed at expanding joint efforts at cyber defense, particularly in connection with Russia. ([Ukrainian and Polish Governments signed a memorandum of cooperation in the cybersecurity field \(mailchi.mp\)](#))

August 22, 2022 – (Date approx.) Nataliia Pinchuk, an adviser to the State Service for Special Communications and Informational Protection of Ukraine (SSSCIP), contributes to a blog for the European Digital Diplomacy Exchange, commenting on Ukraine’s efforts to hold its own in “the very first cyberwar in the world’s history.” She attributes the country’s success to transparency; addressing the needs of critical “audiences,” including people in combat zones; and the role of the international community. ([Digital Diplomacy on Guard of the Country’s Security - European Digital Diplomacy Exchange \(bedigitaldiplomat.com\)](#))

August 22, 2022 – A piece in Foreign Policy underscores the importance of the West’s imposition of export controls to constrain Russian behavior. “In a highly coordinated fashion, the United States and 37 other countries imposed a novel and complex regime of export controls against Russia [after its invasion of Ukraine]. These controls severely restrict the export of strategic technologies, including semiconductors, microelectronics, navigation equipment, and aircraft components, to Russia—harking back to the highly successful Western export restrictions that helped isolate, contain, and ultimately defeat the Soviet Union.” ([Technology Controls Can Strangle Russia—Just Like the Soviet Union \(foreignpolicy.com\)](#))

August 23, 2022 – On the eve of Ukraine’s independence day, the U.S. Embassy in Kyiv issues a security alert saying: “The Department of State has information that Russia is stepping up efforts to launch strikes against Ukraine’s civilian infrastructure and government facilities in the coming days. Russian strikes in Ukraine pose a continued threat to civilians and civilian infrastructure.” No other details are



provided. ([Security Alert - U.S. Embassy Kyiv, Ukraine - U.S. Embassy in Ukraine \(usembassy.gov\)](#))

August 23, 2022 – The Justice & Home Affairs Agencies’ Network of nine European countries publishes a joint paper, “Contributing to the EU’s Solidarity with Ukraine.” It itemizes numerous activities by various European official entities including in the IT and cyber realms. ([JOINT PAPER UA final.pdf \(europa.eu\)](#))

August 23, 2022 – Killnet announces: “Guys, we are starting a week-long shift in Moldova.” ([\(20\) CyberKnow on Twitter](#))

August 23, 2022 – Axios posts an item with several links relating to Russia’s curious lack of significant cyberattacks against Ukraine this year. ([Russia's slow-burn cyber war \(axios.com\)](#))

August 24, 2022 – Hackers gain access to dozens of surveillance cameras (with speakers) in Russia and Russian-occupied territories, using them to play pro-Ukrainian music on Ukraine’s Independence Day. ([Russian surveillance cameras hacked to blast pro-Ukraine music \(americanmilitarynews.com\)](#))

August 24, 2022 – President Biden announces “our biggest tranche of security assistance [to Ukraine] to date: approximately \$2.98 billion of weapons and equipment to be provided through the Ukraine Security Assistance Initiative.” Reports indicate the package includes the VAMPIRE (Vehicle-Agnostic Modular Palletized ISR Rocket Equipment) counter-drone system. ([Russian invasion reaches 6 months on Ukraine’s Independence Day - The Washington Post: New \\$3B US military aid package for Ukraine includes VAMPIRE counter-drone systems \(defensescoop.com\)](#))

August 24, 2022 – According to a U.K. government release: “The UK and Ukraine have today announced their intention to pursue a new digital trade agreement to help Ukraine rebuild its economy and protect livelihoods.” The statement adds the move comes after a direct request from Ukraine’s government. ([UK and Ukraine launch talks on digital trade deal to support Ukrainian businesses - GOV.UK \(www.gov.uk\)](#))

August 24, 2022 – The Norwegian defense ministry announces that Norway and Britain will jointly provide Ukraine with micro drones for use against Russian forces. The Teledyne Flir Black Hornet drones, which are used for reconnaissance and target identification, will cost around \$9.26 million. ([Norway, Britain donate micro drones to Ukraine | Reuters](#))

August 24, 2022 – The Atlantic Council posts the views of several commentators on the lessons of the Ukraine war. On cyber, one expert notes the critical, new role of the private sector, stating that “the United States, NATO, and the democratic nations of the Indo-Pacific need to organize appropriate planning and operational collaborative mechanisms with key elements of the private sector to assure effective operation of cyberspace in the event of armed conflict.”

Another observer warns against ignoring the “home front.” “After an initial burst of activity culminating in late April and early May, efforts by the US Department of Homeland Security (DHS) to counter Russia’s hybrid war in the United States appear to have faded—even amid a Russian “avalanche of disinformation,” as the Atlantic Council’s Digital Forensic Research Lab has documented. The last update to the Cybersecurity and Infrastructure Security Agency’s “Shields Up” webpage was dated May 11, and the most recent entry in CISA’s “Russia Cyber Threat Overview” was dated April 20. The last Russia-specific public alert, “Russian State-Sponsored and Criminal Cyber Threats to Critical Infrastructure,” was revised May 9.” ([Six months, twenty-three lessons: What the world has learned from Russia’s war in Ukraine - Atlantic Council](#))

August 24, 2022 – Six months into the war, *Politico* publishes an article concluding that Ukraine “has borrowed heavily from online tactics first pioneered by the Kremlin.” These include: controlling the narrative (a tactic mastered by President Zelenskyy); working to isolate Russia digitally from the outside world (by exhorting Western companies to shut off operations there); creating a hacker army to amplify government operations; cooperate unreservedly with tech companies (Palantir, Clearview AI, e.g.) that utilize big data and AI for military and law enforcement purposes even though their methods that have raised concerns in the West about data privacy. ([How Ukraine used Russia’s digital playbook against the Kremlin - POLITICO](#))

August 24, 2022 – An article published by the Modern War Institute at West Point (with disclaimers) describes “the next variant of Russia’s political warfare” approach. The author writes that “the core DNA of Russia’s contemporary political warfare campaign remains largely unchanged from Soviet tactics and objectives in the Cold War and is unlikely to radically change after Ukraine. It is nonetheless constantly evolving...” ([The Next Variant of Russia’s Political Warfare Virus - Modern War Institute \(usma.edu\)](#))

August 24, 2022 – A group of U.K. academics publishes a study called “Getting Bored of Cyberwar: Exploring the Role of the Cybercrime Underground in the Russia-Ukraine Conflict.” The study is based on analysis of 281,000 web defacement attacks, 1.7 million reflected DDoS attacks, and “441 announcements (with 58K replies) of a volunteer hacking discussion group for two months before and four months after the invasion.” The authors also conducted numerous interviews. Their conclusion is that cyber criminals were initially captivated by the conflict but fairly quickly lost interest; at no time did their attacks amount to anything very serious or sophisticated. “We can find no evidence of high-profile actions of the kind hypothesised by the prevalent narrative. The much-vaunted role of the ‘IT Army of Ukraine’ co-ordination group is mixed; the targets they promoted were seldom defaced although they were often subjected to DDoS attacks. Our main finding is that there was a clear loss of interest in carrying out defacements and DDoS attacks after just a few weeks.” ([2208.10629.pdf \(arxiv.org\)](#))

Late August 2022 – (Date approx.) According to a digital rights monitoring group, Roskomsvoboda, Russia has shut off access to almost 7,000 websites, including sites belonging to independent media and human rights organizations. ([Ukraine war: Russians kept in the dark by internet search - BBC News](#))

August 25, 2022 – Effects from the Ukraine war have reached as far as the dark web, changing the way many of its inhabitants behave, according to a former U.S. government operative interviewed by *The New Statesman*. Whereas before the war a “gentleman’s agreement” frowned on attacks against members of the Commonwealth of Independent States (consisting of former Soviet republics like Ukraine), that code has now been widely breached, starting with the pro-Kremlin group Conti. Another expert suggests that the dark web is also sharpening the conflict because it makes dissemination of malicious tools and training easier and less risky. ([How the war in Ukraine is reshaping the dark web - New Statesman](#))

August 22-28, 2022 – Montenegro is hit by several hacker strikes, including one a week earlier, according to the National Security Agency (ANB). Outgoing Prime Minister Dritan Abazovic calls it a “very serious attack” that involved the police directorate and Ministry of Defence as well as the ANB. According to the wording of a news report, the ANB says that “such an attack has not been seen anywhere else in the world so far.” Montenegrin officials attribute the hit to Russia although it is later deemed to be a ransomware attack. They continue to believe it ultimately represents retaliation for Montenegro’s support for Ukraine. ([bne IntelliNews - Russia blamed for wave of hacker attacks in Southeast Europe](#); [Montenegro cyberattack: Russian hackers blamed for infrastructure hack \(techmonitor.ai\)](#); [Montenegro blames criminal gang for cyber attacks on government | Reuters](#))

Experts later attribute the attack to Cuba Ransomware. ([Cuba ransomware affiliate targets Ukrainian govt agencies \(bleepingcomputer.com\)](#); see also [Microsoft Word - Cuba Ransomware FLASH NOV11292021\(1\) \(ic3.gov\)](#))

August 26, 2022 – *The Record* posts an interview with Russian hacker Mikhail Matveev, tied to the April 2022 ransomware attack on Washington DC’s Metropolitan Police Department. Matveev, known as “Wazawaka,” makes a couple of observations relating to the Ukraine conflict. For one, he predicts that “ransomware will soon die — not in three years, but sooner. Literally, everything has changed over the last six months. Since the beginning of the special operation in Ukraine, almost everyone has refused to pay. I often encountered people who wrote to me in the chat, “You are a Russian occupier. Be content with \$10k. And we won’t give you more. At least take that.” Convert [or return on investment] has completely fallen in the last six months. It became difficult to work, in general.”

Asked how the war has affected ransomware activities and cybercrime generally, he replies: “It is terrifying, the industry has reorganized. I don’t know if a special operation would have begun, but as far as we all know, Russia began to quietly come into cooperation with the USA regarding cybercrime. I crapped myself and then I was very afraid, I was drinking a lot. I re-read our Constitution and understood that they’ll leave me, damn well, in Russia, but it was scary [editor’s


note: Russia does not have an extradition treaty with the U.S.]. I had already forgotten about the money, and then the special operation had begun. I was fucking happy. Although you know it's dumb to talk about it because my interview will also be read by the citizens of Ukraine, and someone's father could have died, or their child. I started to rejoice, you know, with impunity. But, if it weren't for the special operation, I wouldn't have behaved the way I'm behaving now — I'm even a little ashamed of it." ([An interview with initial access broker Wazawaka: 'There is no such money anywhere as there is in ransomware' - The Record by Recorded Future](#))

August 27, 2022 – Bulgaria's former ruling Gerb party alleges Russian hackers targeted postings on three specific topics on its social media pages. ([bne IntelliNews - Russia blamed for wave of hacker attacks in Southeast Europe](#))

August 26, 2022 – A journalist writing for Bellingcat notes in a Tweet that the Belarus cyber partisans group (@cpartisans) shared a "super useful database" that the investigative group used to track down and expose an apparent GRU illegal. (the grugq newsletter, 8-27-22)

Late August 2022 – Hackers disclose data on almost 44 million customers of the large Russian movie theater chain START. It is reported as the latest in a series of data breaches of Russian companies. (Risky Biz News, 8-29-22)

August 28, 2022 – Ukraine's Defense Ministry tweets a doctored image of a Shiba Inu dog in military dress reacting to the launch of a Lockheed Martin HIMARS rocket. "We usually express gratitude to our international partners for the security assistance. But today we want to give a shout-out to a unique entity – North Atlantic Fellas Organization #NAFO. Thanks for your fierce fight against kremlin's propaganda & trolls. We salute you, fellas! pic.twitter.com/AfDnXf7pfc. — Defense of Ukraine (@DefenceU)" The *Washington Post* leads with this tweet for a story on how Ukraine has been "turn[ing] the trolls on Russia." Noting that "[m]ore than six months in, the war in Ukraine has become a little surreal," the article highlights the antics of NAFO, a wide-ranging group that has made a name for itself as a leading troller of the Kremlin and its allies. ([With NAFO, the North Atlantic Fellas Organization, Ukraine turns the trolls on Russia - The Washington Post](#))

August 29, 2022 – Ukraine launches a major counteroffensive in Kherson Oblast. A week later, wounded Ukrainian soldiers describe heavy losses sustained and a "yawning technology gap" compared to Russian forces. The latter's Orlan tracking drones flew more than a kilometer overhead, making it impossible to hear them. Counter-battery radar systems were effective at locating Ukrainian units and Russian hackers managed to commandeer and neutralize Ukrainian drones. A Twitter user notes the experience reflects "the limits of COTS [commercial off-the-shelf] solutions to asymmetry." ([Wounded Ukrainian soldiers tell of heavy losses in push to retake Kherson - The Washington Post](#); (4)  [мара-яга](#))



August 30, 2022 – The APT group Trident Ursa (aka Gamaredon, UAC-0010, Primitive Bear, Shuckworm), attributed to the FSB, makes an unusual – and ultimately unsuccessful – attempt to compromise an unidentified large petroleum refining company in an unnamed NATO member state. This is according to Palo Alto Network’s Unit 42.

([Russia’s Trident Ursa \(aka Gamaredon APT\) Cyber Conflict Operations Unwavering Since Invasion of Ukraine \(paloaltonetworks.com\)](#))

August 30, 2022 – The Atlantic Council posts “Early lessons from the Russia-Ukraine war as a space conflict.” The report by David T. Burbach calls the Ukraine war “a potential harbinger of the future” and notes four preliminary lessons. “First, despite having no indigenous space capability, Ukraine has made effective battlefield use of space-based communications and intelligence, surveillance, reconnaissance (ISR) assets from US and European commercial providers. Second, for all the attention on kinetic anti-satellite (ASAT) weapons, Russian counterspace attacks have been limited to the cyber domain—achieving some success and causing collateral damage in NATO countries. Third, commercial space will only grow in importance in conflicts, while policy makers in Western countries have yet to make clear when and how they would protect commercial assets. Last, Russia is gaining surprisingly little advantage from its space capabilities, reflecting the long-term weaknesses of the Russian space industry—weaknesses not shared by China, however.” ([Early lessons from the Russia-Ukraine war as a space conflict - Atlantic Council](#))

August 30, 2022 – [Click Here](#), a production of The Record Media, interviews at length a high-level member of the IT Army of Ukraine who provides an update on the group’s cyber campaign against Russia. The unnamed individual says the group’s circumstances have “changed drastically” since the onset of the war. ([Inside the IT Army of Ukraine, ‘A Hub for Digital Resistance’ - The Record by Recorded Future](#))

August 31, 2022 – The government of Finland has announced a plan to help companies boost their cybersecurity efforts through the issuance of vouchers, according to today’s *Wall Street Journal*. The plan involves funding for cybersecurity training, tools, and tests for companies in critical sectors. While Finnish experts note that cyberattacks have not risen significantly since the Ukraine war began, “we keep our guard up,” said one mobile carrier’s security officer. ([Finland Plans Cyber Funding for Companies Amid Rising Security Threats \(wsj.com\)](#))

August 31, 2022 – Ukraine and Romania sign a Memorandum of Understanding covering a range of joint cyber activities, including best practices in cyber defense; information sharing on cyber incidents; cooperation in new cybersecurity studies; and collaboration in certain unnamed projects. ([Uniting efforts with European countries for safer cyberspace and fending off cyber threats \(cip.gov.ua\)](#))

August-September 2022 – The Russian group Cold River attempts to hack the Brookhaven (BNL), Argonne (ANL) and Lawrence Livermore National Laboratories (LLNL), according to internet records reviewed later by Reuters and five cyber security experts. Hackers create fake login pages and attempt to get nuclear scientists to

reveal their passwords. Reuters is unable to determine the reason for the attacks or whether they are at all effective. ([Exclusive: Russian hackers targeted U.S. nuclear scientists | Reuters](#))

September 2022 – A project known as “I Want to Live,” in Ukraine, sets up a hotline that offers Russians (and Ukrainians who have fought on the Russian side) the opportunity to surrender. By early 2023, the project is fielding 200-300 calls per day, according to a spokesperson. (See January 3, 2023, entry) ([Ukraine offers Russian soldiers a hotline to surrender - ABC News \(go.com\)](#))

September 2022 – In an effort to mitigate the threat from disinformation regarding Ukraine, Google’s Jigsaw unit launches “the largest pre-bunking experiment on social media to date.” It consists of six short videos that run twice in the latter half of 2022 and gains 38 million views in Poland, the Czech Republic, and Slovakia, reaching between 62% and 80% of Facebook users and significant portions of the viewership of other media such as Twitter and TikTok. “The measurable effects of the campaign varied between countries and videos, as well as across the questions asked to determine the effectiveness of the intervention. Ultimately, we found the share of viewers who could correctly identify these misinformation tactics increased by as much as 8 percentage points after viewing one of these videos.” ([Defanging Disinformation’s Threat to Ukrainian Refugees | by Jigsaw | Jigsaw | Feb, 2023 | Medium](#))

Early Fall 2022 – Unidentified hackers breach the network of the Wagner Group, gaining access to more than 1 million documents from various entities tied to Yevgeny Prigozhin. The group #Wagnerleaks creates an archive to which journalists representing *Die Welt*, the Dossier Center, *Insider*, *Paris Match*, and *Arte* have access. ([Dossier Center Investigation: Prigozhin's Cyber Troops \(substack.com\)](#))

September 1, 2022 – Hackers exploit a taxi app to order dozens of cabs to a single location in Moscow, bringing traffic to a standstill. According to a spokesman for the cab company, “On the morning of September 1, Yandex Taxi encountered an attempt by attackers to disrupt the service—several dozen drivers received bulk orders to the Fili district of Moscow.” ([Hackers Create Traffic Jam in Moscow by Ordering Dozens of Taxis at Once Through App \(vice.com\)](#))

September 3, 2022 – The Security Service of Ukraine announces it has shut down two bot farms, one in the Kyiv region run by a 24-year-old Zaporizhzhia native currently living in Kyiv, and the other in the Odesa region organized by four local citizens. The sites’ reported aims were to discredit Ukrainian forces and leadership, justify Russia’s invasion, and generally destabilize the country. ([SSU shuts down 2 bot farms that spread destructive content in Ukraine](#))

September 4, 2022 – A tweet by the user @Flash\_news\_ua reads: “The Russians gave the coordinates of a military base to Ukrainian hackers who were posing as attractive

women. IT specialist and founder of the Hackyourmom group Mykyta Knysh told about this in an interview with the Financial Times.” ([\(2\) FLASH on Twitter](#))

September 5, 2022 – President Putin signs a decree instructing the government to ensure Russia’s “technological independence from currently used foreign software.” ([Putin instructs Cabinet to take steps to make Russia independent from foreign software - Russian Politics & Diplomacy - TASS](#))

September 6-8, 2022 – A suspected Turla Team operation (tracked by Mandiant as UNC4210) distributes malware to users in Ukraine. When the event is written up months later, Mandiant VP John Hultquist tweets: “Some of [this] may feel familiar to those of you who remember the Agent.BTZ/Operation Buckshot Yankee days. USB proliferation is back, but the twist here is they let someone else do the proliferating.” Turla is seen as one of Russia’s more capable hacker groups but has been mostly inactive during the Ukraine war, according to reports. ([Turla: A Galaxy of Opportunity | Mandiant](#); [\(21\) John Hultquist on Twitter](#); [Notorious Russian hacking group appears to resurface with fresh cyberattacks on Ukraine - CyberScoop](#))

September 6, 2022 – A DDoS attack shuts down some Japanese government and private sector websites for several hours. Killnet claims involvement, announcing on Telegram a “declaration of war on the Japanese national government as a whole.” ([Pro-Russia hackers claim to have temporarily brought down Japanese govt websites - Asia News Network](#))

September 6, 2022 – The *Wall Street Journal* publishes an article describing ways in which the Ukraine war has produced deeper international cooperation on cyber defense, overcoming entrenched differences over technology policy. Former Obama official Chris Painter calls it “a new era of cyber cooperation between the U.S. and Europe.” ([Russia’s War on Ukraine Deepens International Cyber-Defense Cooperation - WSJ](#))

September 6, 2022 – Ukrainian hacker “Herm1t”, once an antagonist of Ukrainian security authorities, tells *The Record* the story of how, when Russia invaded Crimea in 2014, he began to organize groups to target Russia through cyber. His account is an example of the phenomenon of private hackers working alongside the governments they once exasperated. ([An interview with Ukrainian hacker 'Herm1t' on countering pro-Kremlin attacks - The Record by Recorded Future](#))

September 6-9, 2022 – At the Kyiv Tech Summit, Ethereum Founder Vitalik declares that “Ukraine could well become the next Web3 hub.” “A country can become a Web3 hub if its citizens are actively interested in this technology and decide to make a major contribution to its development ... Ukraine has both the capabilities and the determination to do this.” ([Binance partners with Ukrainian supermarket chain to accept crypto through Pay Wallet \(cointelegraph.com\)](#))

September 7, 2022 – Google’s Threat Analysis Group (TAG) reports it is tracking “an increasing number of financially motivated threat actors targeting Ukraine whose activities seem closely aligned with Russian government-backed attackers. This post provides details on five different campaigns conducted from April to August 2022 by a threat actor whose activities overlap with a group CERT-UA tracks as UAC-0098 ... Based on multiple indicators, TAG assesses some members of UAC-0098 are former members of the Conti cybercrime group repurposing their techniques to target Ukraine.” ([Initial access broker repurposing techniques in targeted attacks against Ukraine \(blog.google\)](#))

September 7, 2022 – Albania cuts diplomatic relations with Iran after a ransomware attack in the latter part of July attributed to the Islamic Republic by Mandiant. Ukraine’s Viktor Zhora tweets support for Albania’s decision, the first known instance of a government severing official ties over a cyber incident. (*The Washington Post*, The Cybersecurity 202, 9-8-2022)

September 7, 2022 – A media report today describes the experiences of Ukraine’s biggest mobile phone network, Kyivstar, with a customer base of approximately 26 million users, in fending off Russian targeting. *Politico* reports that in addition to facing physical strikes, phishing attacks on company networks have tripled and DDoS events have doubled, among other developments. But Kyivstar’s mobile services have not been badly hit overall, according to the company. *Politico* notes that the U.S. government is closely observing the ongoing “battle” for lessons in protecting vulnerable infrastructure. Kyivstar attributes its success to added security measures, including having employees work from occupied territories, as well as help from the Ukrainian government and “citizen counter-hackers” like the IT Army. “Part of our success is because we are forcing Russians to defense,” a company official said, adding that the IT Army has been “creating this hassle on [the Russian] side, and it’s making them more weak because of this.” The article notes that it is “unclear how much of a priority targeting telecommunications is for Russia as it concentrates on gaining and holding ground in Ukraine.” ([Ukraine’s largest telecom stands against Russian cyberattacks - POLITICO](#))

September 7, 2022 – Killnet tweets “Today we officially declare war on the Japanese government!” ([\(4\) CyberKnow on Twitter](#))

September 8, 2022 – A media report mentions the U.S. military “is paying close attention” to the use of drones in the Ukraine war, which provide invaluable intelligence on enemy operations and tactics as well as help guide attacks but are also “terrifying” to soldiers on the ground. Air Force Deputy Chief of Staff Lt. Gen. Clinton Hinote says that ground commanders are reporting that drones are “the thing they are most concerned about.” ([What Ukraine drone videos tell us about the future of war \(theruck.news\)](#))

September 8, 2022 – SpaceX sends a letter to the Pentagon saying it can no longer afford to fund Starlink services in Ukraine on the current basis and asking the Defense



Department to take over military-related uses of the system. This is according to documents obtained by CNN. SpaceX estimates the cost for the rest of 2022 at more than \$120 million and nearly \$400 million for the next 12 months. ([Exclusive: Musk's SpaceX says it can no longer pay for critical satellite services in Ukraine, asks Pentagon to pick up the tab | CNN Politics](#))

September 8, 2022 – The nonpartisan Center for European Policy Analysis (CEPA) publishes a lengthy report by Andrei Soldatov and Irina Borogan presenting a history and breakdown of Russia's "cyber landscape," including an account of the development of cyber operations in the Soviet Union and Russia and a description and analysis of the Kremlin's command-and-control structures. The system is "a remarkably fluid and informal" one coordinated at the level of the Presidential Administration and the Security Council, as opposed to a more traditional, military-dominated structure. ([Russian Cyberwarfare: Unpacking Kremlin Capabilities - CEPA](#))

September 9, 2022 – Ukrainian officials and other cyber experts speaking on the last day of the annual Billington Cybersecurity Summit in Washington D.C. offer insightful commentary on the war, CyberWire reports.

Mykhailo Fedorov, vice prime minister and minister of digital transformation of Ukraine, tells the audience the first lesson of the conflict is that Russian power – kinetic and cyber – has generally been overestimated. "We've shown the whole world that Russia is not the powerful state everyone thought it was." "They're not the second-best army in the world, and they're not the best hackers in the world, either." Fedorov mainly credits Ukrainian defenses, especially the IT Army, which altogether he says have blunted about 98% of daily cyberattacks. The volunteer group's biggest contribution, he says, has been in combating Russian disinformation and propaganda.

Cyberwire continues: "Not only are Russian channels of disinformation being disrupted, and Russian media hijacked to display protest against the war, but the IT Army has also been engaged in delivering news to Russians that their government would rather not receive. The IT Army is also collecting evidence of war crimes. 'We know the names of all the looters,'" Fedorov reports.

Ukraine's deputy minister of digital transformation, Georgii Dubynski, tells conference-goers that Ukraine noticed Russian preparations for the war "as early as October and November" as the Russian government "began trying to enroll hackers" from the GRU, SVR, and FSB. "We didn't believe [war] would come, but we were a little bit ready." He adds that the IT Army has been Ukraine's "secret ingredient," providing a crucial offensive cyber capability that the government lacked. "They receive their targets through the Telegram channel, openly," he notes.

Cyber expert Dmitri Alperovitch adds that it is too soon to draw final conclusions about the ongoing conflict. He does note his surprise that Russia did not do more to try to take down Ukraine's Internet, calling this an "enormous failure" that allowed Ukraine to tell its story. He says Ukraine's ability to modernize its digital capacity has been remarkable. He goes on to add that while hacktivists probably haven't registered any strategic successes, they've been a thorn in Russia's

side, boosted Ukrainian morale, and shown that a combatant can “hack back” without unlimited collateral damage, CyberWire reports.

Dubynski credits Ukraine’s decision to transfer its data to the cloud as another critical move, aided by several western tech firms and governments. “Amazon, Microsoft, Google, Oracle, responded to our call quickly. And other governments offered private clouds, notably Poland and the Baltic states. Collaboration with Big Tech has been very important to us.” (The CyberWire, 9-9-2022)

September 9, 2022 – (Approx.) Ukrainian cyber official Georgii Dubynski tells reporters during the Billington Cybersecurity summit, “We know that Russia is actively using criminals” from other countries. “I believe in part because they have the criminals not only in Russia, but they are also partners, and they are in deep contact with North Korea and Iran and others. We have no proof right now.” ([Congress puts Twitter, social media platforms in the hot seat - POLITICO](#))

September 9, 2022 – For a second time (see August 20 entry), pro-Ukrainian hackers disrupt Russian-controlled TV stations in Crimea to broadcast a speech by President Zelenskyy, Channel 24 in Ukraine reports. ([Zelenskyy's address was shown on television in Crimea - Channel 24 \(24tv.ua\)](#))

September 9, 2022 – President Zelenskyy meets with the head of a Turkish company, Baykar, to discuss plans to build a drone factory in Ukraine. ([Zelenskiy says Turkish drone maker to build Ukraine factory | Reuters](#))

September 10, 2022 – Ukrainian hackers have again hacked Russian TV signals in Crimea, according to a report today in “24 Kanal”. Viewers were shown an address by President Zelensky and given instructions on places to avoid as well as other information. ([В Криму по телебаченню показали звернення Зеленського - 24 Канал \(24tv.ua\)](#))

September 10, 2022 – The *New York Times* reports that some Ukrainian officials expect Russia will go back to conducting large cyberattacks in the wake of Moscow’s inability to counter Ukraine’s eastern offensive by kinetic means. Georgii Dubynski tells the paper: “The next phase is, they will try to defeat our energy and financial sectors. We have seen this scenario before.” ([Ukrainian Officials Drew on U.S. Intelligence to Plan Counteroffensive - The New York Times \(nytimes.com\)](#))

September 11, 2022 – Russian missiles knock out power plants in the Kharkiv and Donetsk regions causing widespread outages, according to senior Ukrainian officials. Ukraine has been expecting critical infrastructure to be targeted but some officials believed Moscow would use cyber methods not kinetic strikes. ([Russian Strikes Cause Blackouts as Ukraine Gains in Northeast - The New York Times \(nytimes.com\)](#))

September 11, 2022 – A report from CyberCube analyses the state of cyber activity in the Ukraine war after six months. The report describes a significant escalation of the use of wiper malware by Russian actors and assesses Moscow's interest in developing an independent Internet network. William Altman of CyberCube comments: "A Russian sovereign internet has several potential implications for cyber activity. Rival nations will find it more difficult to acquire cyber threat intelligence on threat actors operating from inside Russia, and might resort to more drastic measures to achieve this goal, potentially causing collateral damage. Furthermore, there is a potential for future 'collaboration' between Russian, North Korean and Chinese internets, which would increase threat actors' ability to launch attacks." ("Ukraine Cyber War Update: Spotlight on Activity Six Months Later," 9-11-2022; [CyberCube: Russia's Sovereign Internet Creates Security Risks With Implications for Cyber \(Re\)Insurance While War in Ukraine Develops \(apnews.com\)](#))

September 12, 2022 – Security firm Akamai reports that an unnamed client victimized earlier in the summer (see July 21, 2022, entry) has continued to be "bombarded relentlessly with sophisticated denial-of-service (DDoS) attacks," calling the incident a "new European packets per second (pps) DDoS record." ([Record-Breaking DDoS Attack in Europe | Akamai](#))

September 13, 2022 – A senior U.S. intelligence official briefs reporters on a new U.S. intelligence review that concludes Moscow has covertly spent at least \$300 million on foreign political entities and candidates as part of a massive influence campaign since 2014. ([Russia spent millions in secret global political campaign, U.S. says - The Washington Post](#))

September 13, 2022 – Undersecretary of Defense for Policy Colin Kahl tells a virtual meeting of the National Security Council that he has ordered a review of recently reported online psychological operations conducted by U.S. military commands that are causing concerns in parts of the U.S. government – notably the White House – about the use of controversial tactics in the information domain. (See also July-August 2022 entry.) The Washington Post reports the story, adding details about previous activities by CENTCOM and other entities going back at least 2-3 years. ([Pentagon reviews psychological operations amid Facebook, Twitter complaints - The Washington Post](#))

September 14, 2022 – *Wired* publishes an account of an interview with Ukraine's Yurii Shchyhol. In part, it reads: "We're now in the third stage of Russia's cyberwar against Ukraine, says Shchyhol—one that's ongoing and perpetrated 'mostly against civilian infrastructure: utilities and companies that render services to civilians, since they failed to destroy in the second phase our communication lines and our ability to keep people abreast of what's going on.' Russia's digital war playbook is similar to its physical warfare strategy, says the cybersecurity chief. 'Our attitude remains the same,' he says. 'We treat them as criminals trying to destroy our country, invading it on the land but also trying to disrupt and destroy our lifestyle in cyberspace. And our job is to help defend our country.'"

The article continues: “One thing that helped Ukraine learn Russia’s cyber MO was creating a database of attributed Russian attacks that were specified to particular hacker groups. Shchyhol says the Derzhspetsvriazok learned that most groups were sponsored by either Russia’s intelligence service—the FSB, Russia’s post-Soviet successor to the KGB—or the Russian army. Shchyhol refutes the term ‘hactivist’ when used in relation to Russia. ‘A hactivist is a person who does it from the generosity of his heart, free of charge,’ he says. ‘These guys are sponsored by the state and receive a mandate to perpetrate crimes.’ Knowing who was behind the attacks helped, Shchyhol says. ‘By virtue of realizing who is attacking us, it allowed us to be better and more successfully get prepared to repel those attacks,’ he says.” ([Ukraine’s Cyberwar Chief Sounds Like He’s Winning | WIRED](#))

September 15, 2022 – The European Commission presents a proposed new Cyber Resilience Act, billed as the first of its kind, aimed at introducing cybersecurity requirements for digital products. ([State of the Union: New EU cybersecurity rules \(europa.eu\)](#))

September 15, 2022 – Rep. Jim Langevin, D-R.I., chairman of the House Armed Services subcommittee on cyber, innovative technologies and information, discusses USCYBERCOM’s “hunt forward” activities at DefenseScoop’s DefenseTalks conference. “Working with our partners and allies ahead of time in hunt-forward operations that we’re involved with, I believe that that has helped us significantly to be prepared for pushback against Russia in the war in Ukraine ... I think [that’s] a significant reason why we haven’t seen more effective cyber operations on the part of Russia both in Ukraine and maybe any blowback we might have experienced here in the United States.” ([US cyber teams prepped Eucom's networks for potential Russian attacks prior to Ukraine invasion \(defensescoop.com\)](#))

September 15, 2022 – Cisco Talos reports on a new and ongoing malware campaign against Ukrainian targets attributed to the Gamaredon APT, which has ties to Russia. ([Gamaredon APT targets Ukrainian government agencies in new campaign \(talosintelligence.com\)](#))

Mid-September 2022 – A senior Ukrainian official warns of anticipated “concerted” Russian cyberattacks in the next few months, according to a media report. (*Politico*, “Weekly Cybersecurity,” 9-19-2022)

September 2022 – Cybersecurity firm Recorded Future begins a hiring blitz in Ukraine aimed at doubling its presence in the country before 2025. The bulk of new hires will consist of software developers and engineers, as well as threat intelligence analysts “who will study dark web forums for signs of attacks and share intel with their customers,” Axios reports. Recorded Future’s clients are government agencies and a few critical infrastructure companies, Recorded Future’s CEO Christopher Ahlberg tells Axios. “[W]e just love the quality of the work” of the current Ukrainian staff, Ahlberg adds. ([Cyber diplomacy reimaged \(axios.com\)](#))



September 2022 – Russian human-resources company Ventra conducts a survey just prior to Russia’s announcement of a new, large-scale conscription for the war in Ukraine. Even before Vladimir Putin announces a large call-up of reservists (see September 21 entry), the poll finds that 25% of Russian IT are thinking about leaving the country and that 6% have already left in 2022. This backs up another survey during the summer by the Russian Association for Electronic Communications, which finds that 21% of tech workers are thinking about exiting Russia. ([Departure of Tech Workers Weighs on Russian Economy - WSI](#))

September 16, 2022 – Binance Ukraine partners with Ukrainian supermarket chain Varus to enable grocery purchases through Binance Pay Wallet. ([Binance partners with Ukrainian supermarket chain to accept crypto through Pay Wallet \(cointelegraph.com\)](#))

September 19, 2022 – The IT Army announces on Telegram that it has hacked the website of the Wagner Group, a private militia run by Putin ally Yevgeny Prigozhin. “We have all personal data of mercenaries! Every executioner, murderer and rapist will be severely punished. Revenge is inevitable!” ([Telegram: Contact @itarmyofukraine2022](#))

September 20, 2022 – (Date approx.) The Atlantic Council publishes a report on Russian threat actors, the Kremlin’s involvement with them, and ways U.S. policymakers can respond. Written by Justin Sherman, the report begins: “The number of cyber operations launched from Russia over the last few years is astounding, ranging from the NotPetya malware attack that cost the global economy billions, to the SolarWinds espionage campaign against dozens of US government agencies and thousands of companies. Broad characterizations of these operations, such as “Russian cyberattack,” obscure the very real and entangled web of cyber actors within Russia that receive varying degrees of support from, approval by, and involvement with the Russian government.” ([Untangling-the-Russian-Web-Spies-Proxies-and-Spectrums-of-Russian-Cyber-Behavior-1.pdf \(atlanticcouncil.org\)](#))

September 21, 2022 – Vladimir Putin announces Russia will call up 300,000 reservists to help fight in Ukraine. (*Washington Post*, 9-21-2022)

September 21, 2022 – An unidentified drone boat is discovered on a beach near Sevastopol. *Naval News* reports that the “uncrewed surface vessel” (USV) was found outside the harbor entrance to one of Russia’s major naval bases, about 150 nautical miles from Ukrainian controlled coasts. “The clear implication is that the previously unknown USV is operated by Ukraine,” the article reports, adding that available evidence suggests it is some kind of “explosive boat.” ([Ukraine’s New Weapon To Strike Russian Navy In Sevastopol - Naval News](#))

September 22, 2022 – The *New York Times* publishes a lengthy article based on a leak earlier in 2022 (see April 13 entry) of nearly 160,000 records from the Russian government’s Internet regulator, Roskomnadzor. The Times’ analysis gives a

glimpse into the scale and focus of just one part of the Kremlin's high-tech surveillance network keeping tabs on Russian citizens. ([Inside Russia's Vast Surveillance State: 'They Are Watching' - The New York Times \(nytimes.com\)](#))

September 22, 2022 – As of this date, pro-Russian groups generating funds in cryptocurrency to support paramilitary operations in Ukraine have raised \$400,000 since February, according to TRM Labs. (See various entries above.) ([TRM Analysis: Crypto Fundraising Groups Supporting Russian Battlefield Efforts | TRM Insights \(trmlabs.com\)](#))

September 22, 2022 – *Newsweek* quotes Ukrainian officials as saying their country has become a “test ground for modern cyber weapons.” The article states: “Since the invasion began, the intensity of phishing attacks has increased by 300 percent, DDoS attacks by 200 percent, and malware attacks by up to 400 percent, according to KyivStar – a Ukrainian telecommunications giant heavily involved in securing national networks.” KyivStar CEO Oleksandr Komarov tells the magazine, “Cybersecurity is not only about platforms and tools, it’s also about processes and monitoring.” “You will not win a war in cyberspace,” but “you can create panic, you can affect governance mechanisms.” Komarov does not believe the Russians “have a golden bullet” in reserve, but “I think we should be alert.” ([Russia-Ukraine Cyber War Is 'Test Ground' for NATO \(newsweek.com\)](#))

On October 5, OODA Loop posts an analysis that contests the idea that Ukraine has faced qualitatively new kinds of attacks. While Russia has mounted many disruptive and even destructive assaults the author finds “no fresh thinking” on Moscow’s part. ([OODA Loop - Russia's Cyber Attacks in Ukraine is Less About Testing New Attacks and All About Regime Survival](#))

September 23, 2022 – Ukraine’s security services announce they have “neutralized” a hacker group in Lviv that hacked approximately 30 million private Internet accounts in Ukraine and the European Union, then sold confidential data through the anonymous platform ‘Darknet’. “Their ‘wholesale customers’ were pro-Kremlin propagandists who in turn used the data “to spread fake ‘news’ from the front and create panic.” ([SBU neutralizes hacker group that "hacked" almost 30 million accounts of Ukrainian and EU citizens \(ssu.gov.ua\)](#))

September 23, 2022 – Mandiant releases a report on pro-Russia hackers. “Although some of these actors are almost certainly operating independently of the Russian state, we have identified multiple so-called hacktivist groups whose moderators we suspect are either a front for, or operating in coordination with, the Russian state. We assess with moderate confidence that moderators of the purported hacktivist Telegram channels ‘XakNet Team,’ ‘Infoccentr,’ and ‘CyberArmyofRussia\_Reborn’ are coordinating their operations with Russian Main Intelligence Directorate (GRU)-sponsored cyber threat actors. Our assessment is based in part on the deployment of GRU-sponsored APT28 tools on the networks of Ukrainian victims, whose data was subsequently leaked on Telegram within 24 hours of wiping activity by APT28, as well as other indicators of inauthentic activity by the moderators and similarities

to previous GRU information operations.” ([GRU: Rise of the \(Telegram\) MiniOns | Mandiant](#))

September 23, 2022 – The group Anonymous tweets that it has “hacked the website of the Russian Ministry of Defense and leaked the data of 305,925 people who are likely to be mobilized in the first of three waves of mobilization.” Two days earlier, Vladimir Putin announced a partial military mobilization of 300,000 reservists. ([Details of Over 300,000 Russian Reservists Leaked, Anonymous Claims - Infosecurity Magazine \(infosecurity-magazine.com\)](#))

September 23, 2022 – A media item reports that Ireland, Poland, and the Baltic states are circulating a 9-page list of proposals for clamping down harder on Russia within the EU. *EUobserver* reports that the proposals include cutting off a number of major Russian banks such as Gazprombank from the Swift system, prohibiting diamond sales involving Russia, and banning the use of technology from Kaspersky Lab. Eugene Kaspersky has come under heavy fire for protecting Russian military web assets from DDoS attacks, among other reports. ([Ireland joins EU hawks on Russia, as outrage spreads \(euobserver.com\)](#); [Can Kaspersky survive the Ukraine war? \(cyberscoop.com\)](#))

September 24, 2022 – A Dutch news outlet, *deVolkskrant*, publishes an article about a Dutch former soldier who joined the IT Army of Ukraine, adopting the name Hactic. He takes credit for targeting Aeroflot, among other attacks. (Risky Biz News, 9-28-2022; [Een internationaal cyberleger tegen Rusland met een Nederlander in de hoofdrol \(volkskrant.nl\)](#))

Late September 2022 – Taiwanese semiconductor magnate Robert Tsao pledges about \$20 million to fund civilian military training for Taiwanese citizens to resist disinformation campaigns that would presumably accompany a Chinese invasion of the island. News reports indicate many Taiwanese have been watching the Ukraine war for lessons in this regard. ([Taiwanese citizens prepare for possible cyber war \(axios.com\)](#))

Late September 2022 – Russia begins testing its Tobol electronic warfare system as a means to disrupt Ukraine’s internet access via Starlink, according to a classified U.S. intelligence report obtained by the *Washington Post*. The test reportedly continues for several months but the top-secret assessment, part of the Discord leaks, has no information on what that signifies. ([Russia unveils secretive weapon to target SpaceX’s Starlink in Ukraine - The Washington Post](#))

September 26, 2022 – Ukraine’s Defense Intelligence agency warns: “The kremlin is planning to carry out massive cyberattacks on the critical infrastructure facilities of Ukrainian enterprises and critical infrastructure institutions of Ukraine’s allies. First of all, attacks will be aimed at enterprises of energy sector. The experience of cyberattacks on Ukraine’s energy systems in 2015 and 2016 will be used when conducting operations. By the cyberattacks, the enemy will try to increase the effect

of missile strikes on electricity supply facilities, primarily in the eastern and southern regions of Ukraine. The occupying command is convinced that this will slow down the offensive operations of the Ukrainian Defence Forces. The kremlin also intends to increase the intensity of DDoS attacks on the critical infrastructure of Ukraine's closest allies, primarily Poland and the Baltic states.” ([Invaders Preparing Mass Cyberattacks on Facilities of Critical Infrastructure of Ukraine and Its Allies \(gur.gov.ua\)](#))

September 26, 2022 – Observers notice the first gas leaks from the Nord Stream 2 pipeline. Sometime later, the satellite data monitoring firm SpaceKnow pieces together data from multiple satellite services and reports its finding that two “dark ships ... of a significant size” coming within several miles of the leak sites. “They had their beacons off, meaning there was no information about their movement, and they were trying to keep their location information and general information hidden from the world,” reports Jerry Javornicky, CEO and cofounder of SpaceKnow. The company provides the information to NATO. ([‘Dark Ships’ Emerge From the Shadows of the Nord Stream Mystery | WIRED](#))

September 26, 2022 – Journalist Kim Zetter posts an item indicating that senior Ukrainian cyber official Victor Zhora now downplays the impact of the February 24 Viasat attack, after initially telling reporters it caused a “really huge losses.” In an interview with Zetter, Zhora now says it was the “opposite.” “I was saying that that *didn’t have* significant impact” (emphasis in original). He adds that the incident “had a serious impact on [the] satellite component of communications” but not on land lines which make up the “primary way of communications in armed forces.” (See also February 24 and Early March entries.) ([Viasat Hack “Did Not” Have Huge Impact on Ukrainian Military Communications, Official Says \(substack.com\)](#))

Late September 2022 – Elon Musk reportedly tells political analyst Ian Bremmer that he recently refused a Ukrainian Defense Ministry request to activate Starlink in Crimea “given the potential for escalation” of the conflict, in Bremmer’s words. This follows a reported conversation between Musk and Vladimir Putin, which both of the latter deny happened. Bremmer writes later that Musk told him Putin threatened to use nuclear weapons if Ukraine tried to recapture Crimea. ([Elon Musk Blocks Starlink in Crimea Amid Nuclear Fears: Analyst \(businessinsider.com\)](#))

Late September 2022 – The Belfer Center releases “National Cyber Power Index 2022,” its second annual report, described as a “snapshot of the current status of ... thirty countries.” The United States, China, and Russia occupy the top three slots while Ukraine moves up from 29<sup>th</sup> to 12<sup>th</sup> since 2020. ([National Cyber Power Index 2022 | Belfer Center for Science and International Affairs](#))

September 27, 2022 – Meta reports that it has identified and shut down a large Russian disinformation network involving over 60 websites. The operation aimed at disseminating Russian propaganda by mimicking mainstream media sites and populating them with false information. More than 1,600 fake Facebook accounts



were also involved, targeting Germany, Italy, France, the U.K. and Ukraine. A media account notes: “The findings highlighted both the promise of social media companies to police their sites and the peril that disinformation continues to pose.” ([Meta disables Russian propaganda network targeting Europe | AP News](#))

September 27, 2022 – (Date approx.) Microsoft blocks access to Windows 11 updates to users in Russia, according to a report today in the Russian news outlet *Izvestia*. ([Closed windows: Microsoft has blocked Windows 11 updates for Russia | Articles | News \(iz.ru\)](#))

September 27, 2022 – *Lawfare* posts an article that delves into the issue of “patriotic hacking.” Authors Jason Healey and Olivia Grinberg spotlight the actions of Ukraine’s IT Army as a case in point and argues that the group “challenges existing norms on civilian participation in war, the applicability of laws of armed conflict to cyberspace, and state responsibility for cyber offenses.” The article points up the risks of this kind of hacktivism and offer several recommendations for how states should conduct themselves, starting with refusing to allow their territory to be used for “internationally wrongful acts.” ([‘Patriotic Hacking’ Is No Exception - Lawfare \(lawfareblog.com\)](#))

*Lawfare* later posts another piece that takes a very different position, arguing that the Healey/Grinberg article “overstates the role of international norms generally and norms related to cyberspace specifically as they relate to armed conflict ... Ukraine’s decision to disregard cybersecurity norms vis-a-vis Russia under current circumstances is wholly consistent with international law and does not represent a failure to live up to its normative commitments in any way.” ([Cyber Norms in the Context of Armed Conflict - Lawfare \(lawfareblog.com\)](#))

September 28, 2022 – Lindy Cameron, chief executive of the U.K.’s National Cyber Security Centre, tells the Chatham House security and defence conference the NCSC has “not been surprised by the volume of Russian offensive cyber operations, nor have we been surprised by their targeting,” a view based on decades of studying Russian cyber doctrine. She says Russia’s operations have not all aimed at having major impact, mainly targeting the Ukrainian government’s ability to communicate, the financial system, and public concerns. It is “a visible example of Russian doctrine in action: using cyber operations as a tool in support of wider military objectives.”

“But for me, in many ways the most important lesson to take from the invasion is not around the Russian attacks — which have been very significant and, in many cases, very sophisticated. It is around Russia’s lack of success,” she tells the conference. “Try as they might, Russian cyber attacks simply have not had the intended impact,” thanks to Ukraine’s own efforts aided by private sector and international cooperation. “If the Ukrainian cyber defense teaches us a wider lesson – for military theory and beyond – it is that in cybersecurity, the defender has significant agency. In many ways you can choose how vulnerable you can be to attacks.”

As for the future, anything is possible. “In response to significant battlefield set-backs, in the last week we have seen Putin react in unpredictable ways... There

is still a real possibility that Russia could change its approach in the cyber domain and take more risks — which could cause more significant impacts in the UK.” ([Russia waging ‘most sustained and intensive cyber campaign on record,’ NCSC CEO says - The Record by Recorded Future](#))

September 28, 2022 – USCYBERCOM Executive Director David Frederick addresses a GovCon Wire event in which he discusses his agency’s “hunt forward” operations in Europe in 2022, among other topics. ([USCYBERCOM Executive Director David Frederick Outlines Cyber Threats & Highlights Importance of Industry Partnerships - GovCon Wire](#))

September 28, 2022 – CoinDesk reports that the EU will tighten limits on Russian crypto investments in the wake of Moscow’s “sham” independence referenda in occupied regions of Ukraine. ([EU Set to Ban Russian Crypto Payments After ‘Sham’ Referenda \(coindesk.com\)](#))

September 28, 2022 – In an apparent attempt to cash in on the Ukraine war, dozens of online stores in the Netherlands are trying to sell firewood in advance of a possible winter-time energy and heating crisis. Dutch police have received more than 500 reports on the matter. (Risky Biz News, 9-28-2022)

September 28, 2022 – The *New York Times* publishes a lengthy article reproducing and assessing recordings of phone calls home made by Russian soldiers early in the war. The *Times* says it got exclusive access to thousands of recordings, reportedly intercepted by Ukrainian law enforcement. The excerpted conversations almost uniformly feature deeply disgruntled Russian troops complaining to friends and family and revealing an appalling pattern of criminality and misconduct. Although the article comes out in late September, the recordings are limited to calls originating in the western Kyiv suburb of Bucha from about six months earlier (March 2022), when Russian attempts to seize the Ukrainian capital were being bogged down by surprisingly strong Ukrainian resistance. ([‘Putin Is a Fool’: Intercepted Calls Reveal Russian Army in Disarray - The New York Times \(nytimes.com\)](#))

September 28, 2022 – A media report indicates an Israeli tech firm, the Avnon Group, is selling social media mapping and tracking software to Hungary. The Orban government’s intended use of the software is not known but a company official “assumed” it relates to growing tensions within Hungary over the war in Ukraine. ([Israeli firm to sell social media-tracking software to Orban's Hungary | The Times of Israel](#))

September 29, 2022 – NATO issues a brief statement declaring that the damage to the Nord Stream pipelines was the result of sabotage. The statement does not name a perpetrator but warns that the alliance is “committed to prepare for, deter and defend against the coercive use of energy and other hybrid tactics by state and non-state actors. Any deliberate attack against Allies’ critical infrastructure would be

met with a united and determined response.” ([NATO - Official text: Statement by the North Atlantic Council on the damage to gas pipelines, 29-Sep.-2022](#))

September 29, 2022 – The International Telecommunication Union elects Doreen Bogdan-Martin as secretary-general of the U.N. organization that works on global connectivity and sets standards for emerging tech. The longtime U.S. diplomat defeats Moscow-backed Rashid Ismailov, a former high official in Russia’s telecom ministry, attaining 139 out of 172 votes. The vote is seen by some observers as a critical referendum pitting Western visions of a relatively free global Internet against the goal of Russia and China to guarantee the right of individual states to regulate the Internet within their national boundaries. Morell cites Russia’s behavior in Ukraine as part of his argument. ([Member States elect Doreen Bogdan-Martin as ITU Secretary-General; Opinion | A free and open internet could hinge on this obscure election - The Washington Post](#))

Further analysis comes in a subsequent article on the website of *The Wire* which concludes: “Bogdan-Martin’s decisive victory suggests that Russia’s war with Ukraine has alienated many of the other countries that it might once have been able to muster to support a more government-centric model of internet governance. Where once Russia was able to rally nearly half of the ITU countries with accusations that the US is too powerful when it comes to running the internet, now the vast majority of those same countries seem to prefer US leadership to a Russian alternative – and that’s a shift that could have profound implications for the future of the internet and who gets to run it. It’s a striking example of how Russia’s invasion of Ukraine is thwarting its international ambitions related to the internet, an outcome that may well frustrate China, Russia’s long-time ally in rallying ITU members to oppose US leadership.” ([How Russia’s Ambitions in Ukraine Are Thwarting Its Plans to Lord Over the Internet \(thewire.in\)](#))

September 29, 2022 – Finland’s Security Intelligence Service (SUPO) publishes its “National Security Overview 2022” in which it notes: “Future NATO membership will make Finland a more interesting target for Russian intelligence and influence operations. One target of particular interest will be the formulation of policy in a militarily allied Finland. Russia’s assessment of what kind of NATO member Finland is becoming determines the aims and methods of influence operations. Finland is portrayed as a member of a hostile alliance, whose location in the near vicinity of Russia exemplifies the threat of NATO enlargement, a narrative disseminated by the Russian regime.”

The report continues: “Russian reactions to Finland’s NATO accession process have been restrained for the time being, and Finland has not been subject to any extraordinary influencing in the course of policymaking, and of the ratification round that followed the accession announcement.” In addition, “Russia will probably focus its intelligence operations increasingly on the cyber environment. It is also probable that the threat of business espionage will grow as Russia feels the need to begin substitute manufacturing of cutting-edge technology. Russia may seek to acquire NATO-related intelligence through Finland.”

In a press release accompanying the new overview, SUPO Director Antti Pelttari comments: “We consider it highly likely that Russia will turn to the cyber environment over the winter.”

China represents the other major threat to Finland, the overview says. “China continues to target active intelligence operations on Finland, in the form of both human intelligence and cyber espionage efforts. Examples of intelligence targets include cutting-edge technology, the Arctic region and national policymaking.” However, the Russian invasion of Ukraine has not significantly affected Chinese intelligence and influencing operations directed at Finland. ([Foreign intelligence and influence operations | Supo](#); [National Security Overview: Russian intelligence changes approach | Supo](#))

September 30, 2022 – *Lawfare* publishes a lengthy analysis by Susan Landau entitled, “Cyberwar in Ukraine: What You See Is Not What’s Really There.” Introducing the piece, Landau writes: “This war has demonstrated strategic cyber issues below the surface, including the failure of effective cyberattacks occurring alongside kinetic offensives, Russia’s long-term use of information warfare, and effective collaboration between U.S. industry and the U.S. government in preventing the worst of the cyberattacks. These have important long-term implications for the international defense strategies of the United States and other Western democracies.” ([Cyberwar in Ukraine: What You See Is Not What’s Really There - Lawfare \(lawfareblog.com\)](#))

End September 2022 – (Date approx.) Undersecretary of Defense for Acquisition and Sustainment William LaPlante meets with allied counterparts to discuss how to build each country’s industrial base as part of the continuing effort to support Ukraine as well as get ready for upcoming wars. The meetings are later reported in the context of a broad lesson-drawing effort from Russia’s occupation of Ukraine. As one account frames it: “Ukraine’s savvy application of different technologies in the ongoing conflict sparked by Russia’s invasion is informing how Pentagon leaders are thinking about and approaching the development of new and emerging capabilities for future wars. It’s also highlighting the need for robust support from America’s defense industrial base to sustain high-tech fights.” ([DOD counting on 'depth of support' from defense industrial base to keep up with evolving warfare \(defensescoop.com\)](#))

September-December 2022 – During this period, according to a report published in December by Ukraine’s SSSCIP, the number of Russian cyberattacks actually dipped but the bulk of them targeted “civil infrastructure” rather than military sites. The number of incidents reached 2,100 for the year with more than 1,500 occurring since the February invasion, the report says. “Cyberattack intensity remains at a certain constant level.” The document, prepared with support from the EU and USAID (which include a disclaimer about not subscribing to the authors’ views), runs through various activities and statistics for the year and offers analysis and prescriptions for action – for example: “There is no doubt that Russian [sic] cyber terrorism is not limited to Ukraine, as the same groups threaten virtually the entire



civilized world. That is why design and implementation of a new contributory system of cyberspace security for the whole civilized world is a priority task for today.” ([SSSCIP Digest 2022 09 12 ENG.pdf \(mcusercontent.com\)](#))

September-December 2022 – During this period, according to a later ESET report, the Russia-aligned APT group Callisto, also known as COLDRIVER or SEABORGIUM, “has been busy registering dozens of domains that are then used to conduct spearphishing attacks in order to steal webmail credentials. The size of their network infrastructure probably explains why the group recently received public attention including blogposts by SEKOIA.IO, PwC and Reuters. Some domains registered by the group suggest Callisto may have targeted the US satellite technology company Blue Sky Network ... and the Polish defense company UMO.” ([eset apt activity report t32022.pdf \(welivesecurity.com\)](#))

Fall 2022 – A new Trojan called CryWiper strikes numerous judicial and mayoral sites in Russia, Kaspersky reports later. The malware pretends to be ransomware but instead of encrypting data for subsequent extortion purposes it destroys it, the company concludes, adding “this was not a developer’s mistake.” ([Вайпер CryWiper атакует притворяется шифровальщиком | Securelist](#); [Risky Biz News: CryWiper hits Russian courts and mayor offices in data-wiping attacks \(substack.com\)](#))

Early October 2022 – Killnet claims responsibility for hits against several state government websites in the United States. ([US Airport Websites Hit by Suspected Pro-Russian Cyberattacks | SecurityWeek.Com](#))

October 2022 – Kaspersky identifies “an active infection of government, agriculture and transportation organizations located in the Donetsk, Lugansk, and Crimea regions. Although the initial vector of compromise is unclear, the details of the next stage imply the use of spear phishing or similar methods.” ([Bad magic: new APT found in the area of Russo-Ukrainian conflict – Securelist](#))

October 2022 – (Date approx.) GroupSense releases *The Cyber Warfare Report: A look at the first eight months of cyber warfare waged against Ukraine*. The report briefly breaks down countries attacked, sectors targeted, and hacktivist groups. It predicts that “many methods and attacks that occur during the conflict won’t be discovered for years to come.” The document lists several entities identified with Ukraine: the IT Army of Ukraine, AgainstTheWest/BlueHornet, Network Battalion ‘65, DoomSec, and GhostSec. It also names several Russian groups, including Killnet, Zarya, NoName057(16), Beregini, and Nemezida. ([The Cyber Warfare Report.pdf \(groupsense.io\)](#); The Cyberwire, 3-1-2023)

October 2022 on – According to a later media report, “Since October [2022], when Russia changed its tactics to target civilians and their infrastructure, internet connectivity has become far more unstable. Several times, it’s dropped below 50 per cent, measured at the national level. ‘[This] means that certain locations must have had almost a complete loss of electricity or internet connection,’ Dr. Simon Angus,

director of the IP Observatory tells ABC Australia. ([The battle to keep Ukraine connected to the internet amid Russian missile attacks - ABC News](#))

October 2022 – ESET detects a previously unknown malware which it calls NikoWiper, which was used to target a Ukrainian energy firm and which ESET attributes to Sandworm. As ESET notes, the attack “happened around the same period that the Russian armed forces targeted Ukrainian energy infrastructure with missile strikes. Even if we were unable to demonstrate any coordination between those events, it suggests that both Sandworm and the Russian armed forces have the same objectives.” ([eset apt activity report t32022.pdf \(welivesecurity.com\)](#))

October 2022 – ESET also uncovers new versions of CaddyWiper and HermeticWiper deployed in Ukraine, as well as an instance of Prestige ransomware which was used to attack logistics companies in Ukraine and Poland (also reported by Microsoft). ESET attributes all three to Sandworm. ([eset apt activity report t32022.pdf \(welivesecurity.com\)](#))

October 2022 – A Russian company named OpZero raises its price for Signal RCE exploits, reports *The Info Op* from the grugq. Because Ukraine’s military and government use Signal extensively, grugq notes, this is potentially a “huge exposure.” ([Russian Oday thirst traps - by the grugq - The Info Op \(substack.com\)](#))

October 2022 – Hackers mount DDoS strikes against 80 Moldovan state computer systems, with modest success. ([Moldova’s government hit by flood of phishing attacks - The Record from Recorded Future News](#))

October 2022 – Sometime this month, CIA Director William Burns visits Ukraine where he reportedly meets with President Zelensky. ([October 26, 2022 Russia-Ukraine news \(cnn.com\)](#))

October-November 2022 – The journal *Survival* publishes a lengthy analysis of “The Cyber Dimension of the Russia-Ukraine War” in its October-November issue. Author Marcus Willett, a former career GCHQ official who helped design U.K. cyber strategy. (For a link to the full article, see: [The Cyber Dimension of the Russia-Ukraine War \(iiss.org\)](#))

October-December 2022 – According to a later report by European cybersecurity firm Thales, “In the third quarter of 2022, Europe was dragged into a high-intensity hybrid cyber-war at a turning point in the conflict, with a massive wave of DDoS attacks, particularly in the Nordic and Baltic countries and Eastern Europe. Cyber is now a crucial weapon in the arsenal of new instruments of war, alongside disinformation, manipulation of public opinion, economic warfare, sabotage and guerrilla tactics. With the lateralisation of the conflict from Ukraine to the rest of Europe, Western Europe should be wary of possible attacks on critical infrastructure in the short term if the conflict continues to accelerate.” ([From](#)

[Ukraine to the whole of Europe:cyber conflict reaches a turning point | Thales Group](#))

October-December 2022 – Russian-authored disruptive cyberattacks against Ukraine surge during this period, according to Mandiant. While “earlier attempts relied on quick turnaround operations using CADDYWIPER variants,” attacks in the last quarter of 2022 “saw GRU clusters deploying ransomware variants on targeted networks.” By contrast, attacks in the first quarter of 2023 do not appear to maintain the same level of intensity. ([Faltering against Ukraine, Russian hackers resort to ransomware: Researchers - Breaking Defense](#))

October 2, 2022 – Interfax news agency reports that Roskomnadzor has blocked the music streaming platform Soundcloud. The action was taken at the behest of the Russian Prosecutor General's Office “in connection with placement of materials containing false information regarding the nature of the special military operation on the territory of Ukraine,” Interfax reported. ([Russia blocks SoundCloud, citing spread of 'false information,' Interfax reports | Reuters](#))

October 2, 2022 – *Kyiv Post* reports on the National Republican Army (NRA), a group of Russians trying to overthrow the Putin government, who have launched a ransomware attack against a major Russian software development company called Unisoft. NRA members contacted the news outlet to describe their exploit and provide evidence, which *Kyiv Post* says it was able to verify. Unisoft has a number of Russian government clients whose data is reportedly among the information NRA is threatening to make public. The article begins with the statement: “*For the first time in known history, hackers from within Russia have begun a systemized effort to hack Russian government affiliated websites*” (emphasis in original). NRA members told the outlet their main motivation was “Putin needlessly sending our young men to die in an unjust war ...” ([Russian Citizens Wage Cyberwar From Within - Kyiv Post - Ukraine's Global Voice](#))

October 3, 2022 – Elon Musk tweets: “Ukraine-Russia Peace: – Redo elections of annexed regions under UN supervision. Russia leaves if that is will of the people. – Crimea formally part of Russia, as it has been since 1783 (until Khrushchev’s mistake). – Water supply to Crimea assured. – Ukraine remains neutral.” He also posts a poll asking whether the “will of the people” should determine the status of contested parts of Ukraine. The same day, Volodymyr Zelensky tweets a poll of his own in response to Musk’s “insane” query: “Which @elonmusk do you like more? One who supports Ukraine [or] One who supports Russia” ([\(7\) Elon Musk on Twitter: "Also worth noting that a possible, albeit unlikely, outcome from this conflict is nuclear war" / Twitter](#); [\(7\) Володимир Зеленський on Twitter: "Which @elonmusk do you like more?" / Twitter](#))

October 4, 2022 – Killnet posts a message on Telegram hinting that the group is planning a wave of DDoS attacks on U.S. government websites over the next three days, calling the event “USA Offline.” Several U.S. targets are subsequently hit but with little or no

meaningful effect, according to a later analysis on *Lawfare*. ([What Impact, if Any, Does Killnet Have? - Lawfare \(lawfareblog.com\)](#))

October 4, 2022 – The cybersecurity firm Secureworks publishes “2022 State of the Threat: A Year in Review” which reports: “The war against Ukraine has been revealing for Russia’s cyber capabilities. At the outset of the conflict there were wide fears of destructive attacks with wide scale repercussions as was seen with NotPetya in 2017. However, despite a steady cadence of cyber activity directed against Ukrainian targets, some of which is identifiably from Russian government-sponsored threat actors, no widely disruptive attacks have been successful.” The report notes that the “most visible” Russian threat group has been IRON TILDEN. As for China meanwhile, “observed threat activity from Chinese government sponsored groups has targeted both Russia and Ukraine. A notable behavior from these adversaries is the use of ransomware as a smokescreen for intellectual property theft and cyberespionage, rather than for financial gain.” ([2022 State of the Threat Report | Secureworks](#))

October 4, 2022 – Reflecting on the impact of the war on Ukraine’s technology sector and the large number of displaced, highly skilled people behind it, the outlet *rest of world* publishes a lengthy piece, “Coding in a War Zone: Ukraine’s Tech Industry Adapts to a New Normal.” ([Coding in a war zone: Ukraine’s tech industry adapts to a new normal - Rest of World](#))

October 4, 2022 – NATO is reported to be trying to work out better ways to protect undersea critical infrastructure in the wake of the Nord Stream pipeline explosions. ([NATO Puzzles Over How to Shield Vital Undersea Links From Attack - Bloomberg](#))

October 6, 2022 – Iran and Russia agree to a deal in which the Islamic Republic will supply more ballistic missiles and drones to Russian forces. The missiles are said to be Fateh-110 and Zolfaghar models, the drones are the Shahed-136 model. Western and Iranian officials later confirm the arrangement to Reuters. ([Iran agrees to ship missiles, more drones to Russia | Reuters](#))

October 6, 2022 – The European Commission announces its eighth sanctions package against Russia over Ukraine, including a provision to ban “all crypto-asset wallets, accounts, or custody services, irrespective of the amount of the wallet.” This expands the range of services to include IT consultancy, legal advisory, architecture and engineering services. “These are significant as they will potentially weaken Russia’s industrial capacity because it is highly dependent on importing these services.” ([Ukraine: EU agrees on eighth package of sanctions \(europa.eu\)](#))

October 7, 2022 – The IT Army of Ukraine defaces the website of the Collective Security Treaty Organization, the Russia-affiliated group of six post-Soviet states, posting a message congratulating Putin on his birthday. ([Development of the Ukrainian Cyber Counter-Offensive | Trustwave](#))



October 7, 2022 – Since this date, according to Trustwave, “the IT Army of Ukraine has focused on Russian financial institutions and businesses such as Sberbank, Gazprombank, Credit Bank of Moscow, Wildberries, and others.” ( [Development of the Ukrainian Cyber Counter-Offensive | Trustwave](#))

October 7, 2022 – *The Financial Times* today reports Starlink services in formerly Russian-occupied territories of Ukraine have been disrupted; no cause has been determined publicly. Later, CNN reports that early this month Ukrainian officials turned to the British to ask for help in paying the \$2,500 monthly fee SpaceX has been charging to keep each terminal connected. The British reportedly decline. (The CyberWire, 10-11-22; [Ukraine suffered a comms outage when 1,300 SpaceX satellite units went offline over funding issues | CNN Politics](#))

October 7, 2022 – Elon Musk tweets a response to today’s *Financial Times* article; the tweet spotlights costs associated with the deployment of Starlink terminals to Ukraine (see also September 8, 2022, entry). “Bad reporting by FT. This article falsely claims that Starlink terminals & service were paid for, when only a small percentage have been. This operation has cost SpaceX \$80M & will exceed \$100M by end of year.” ([\(9\) Elon Musk on Twitter](#))

October 8, 2022 – A 25-year-old Russian is stopped by Metro police in Moscow and asked for his papers, according to sources who spoke later to the BBC. What makes the incident unusual is that the police officer shows the individual (using the pseudonym Anton in the article) a photo that Anton realizes has just been taken of him inside the Metro station. “A fresh photo, just taken,” he is quoted as saying. The BBC article goes on to describe other instances of Russian use of facial recognition technology to spot people suspected of evading call-up to military service in Ukraine. ([Из метро - на фронт. Как власти Москвы следят за "уклонистами" с помощью системы распознавания лиц - BBC News Русская служба](#))

October 10, 2022 – DDoS attacks hit several major U.S. airport websites including Atlanta, Chicago, Los Angeles, New York, Phoenix and St Louis. This follows the posting of a list of target sites by Killnet. Flight services reportedly are not affected. ([US Airport Websites Hit by Suspected Pro-Russian Cyberattacks | SecurityWeek.Com](#))

This week state government websites in Colorado, Mississippi, and Kentucky go offline, an event for which Killnet also claims responsibility. ([Ongoing US support to Ukraine could prompt Russian cyber escalation in midterms, experts warn | The Hill](#))

October 10, 2022 – Yuriy Zaskoka, head of critical infrastructure protection at Ukraine’s Cyber Police Department, dies as a result of a Russian missile strike in Kyiv, according to the department. ([Внаслідок ракетного удару росії по Києву загинув кіберполіцейський — Департамент Кіберполіції \(cyberpolice.gov.ua\)](#))

October 10, 2022 – Brigadier General Guy Jones of the U.S. Army Futures Command tells attendees at the annual Association of the U.S. Army conference that the Army is

closely observing events in Ukraine and incorporating some of those observations into Project Convergence, described by a media account as a “massive networking-and-technologies exercise.” (PC 22 is taking place from September to November and including foreign participants – from the U.K. and Australian – for the first time.) Jones adds the Army has to be “very cautious not to get the wrong lessons.” ([US Army carefully folding Ukraine info into Project Convergence tests \(c4isrnet.com\); Project Convergence 2022 to demonstrate futuristic joint, multinational warfighting technologies | Article | The United States Army](#))

October 10-11, 2022 – Heavy Russian missile strikes cause numerous casualties as well as power outages across several parts of Ukraine, disrupting internet and mobile communications, according to Cloudflare. On October 10, 84 missiles and 24 drones cause damage to critical infrastructure, schools, and other public facilities, according to reports, causing the worst blackouts since the start of the war and sparking concerns about war crimes. Bellingcat, the *Insider* and *Der Spiegel* subsequently discover the identity of a “secretive group of dozens of military engineers” believed to be behind the targeting of these strikes (see October 24, 2022, entry below). ([Recorded Future; The Remote Control Killers Behind Russia’s Cruise Missile Strikes on Ukraine - bellingscat](#))

October 11, 2022 – A series of ransomware attacks takes place in Ukraine and Poland within an hour of each other, Microsoft reports on Oct 14. A month later, the company identifies the ransomware as “Prestige” and assesses that the group behind the attacks is IRIDIUM, labeled by others as Sandworm (see November 10 entry below). ([Microsoft attributes ‘Prestige’ ransomware attacks on Ukraine and Poland to Russian group - The Record by Recorded Future](#))

October 11, 2022 – Recent Russian strikes against Ukraine’s infrastructure prompt an Australian journalistic inquiry into Ukraine’s greatest vulnerabilities. Experts from defense and other sectors place submarine cables at the top of the list. “About 95 per cent of Australia’s internet traffic flows through underwater fibre optic cables,” according to the *Sydney Morning Herald*. Only around 10 intercontinental cables connect Australia to the world, most of them terminating at Perth or Sydney beaches. Director of the International Cyber Policy Centre Fergus Hanson observes that most of the landing points are not secret. “It’s one of the weird anomalies of the internet, a system built on trust, that’s surprisingly insecure for a system so central to everything we do.” ([Russia-Ukraine war: Western, Australian weaknesses exposed in ‘grey zone’ warfare \(smh.com.au\)](#))

October 11 - GCHQ Director Jeremy Fleming implies to BBC Radio that Britain is on the lookout for “indicators” that Russia might be considering deploying nuclear weapons in the war with Ukraine. ([UK spy agency watching for any signs Russia considering nuclear weapons | Reuters](#))

October 11, 2022 – Political analyst Ian Bremer tweets: “elon musk told me he had spoken with putin and the kremlin directly about ukraine. he also told me what the

kremlin's red lines were." Both Musk and the Kremlin deny it. (This follows a report – see October 7 – that Starlink services have been disrupted in territories formerly occupied by Russia.) The alleged Musk-Putin conversation reportedly took place two weeks earlier.

([https://twitter.com/ianbremmer/status/1579941475613229056?s=61&t=m8ch0zR6w9gH7Ym-0bp2uA&utm\\_source=substack&utm\\_medium=email](https://twitter.com/ianbremmer/status/1579941475613229056?s=61&t=m8ch0zR6w9gH7Ym-0bp2uA&utm_source=substack&utm_medium=email); the grugq newsletter, 10-12-22); [Elon Musk Spoke With Vladimir Putin Before Ukraine Peace Plan Poll: Report \(businessinsider.com\)](#))

October 11, 2022 – CISA's Jen Easterly and NSA/USCYBERCOM's Gen. Paul Nakasone discuss Ukraine and related issues such as the Joint Cyber Defense Collaborative at a Council on Foreign Relations event.

Asked what has surprised him most about the war, Nakasone points to "the fact that we have learned a tremendous amount in terms of, you know, how do we look at cybersecurity and how do we look at it differently?" He credits Hunt Forward teams from U.S. Cyber Command and the Ukrainians themselves for hardening their networks and staying "a step ahead of what the Russians are doing."

Regarding reasons why Russia was not as effective on the cyber front as most people expected, Nakasone comments: "First lesson learned? Presence matters. We learned that again in terms of not only were we able to assist Ukraine in terms of the networks they looked at, but interestingly enough as you have a presence on the ground all the malware that's coming in, it's coming to this team to say: Hey, can you help us? And so while I would certainly not say that's the key reason, I think it's a contributing factor."

Expanding on lessons, Nakasone mentions the importance of "being able to be there and understanding what's going on on the ground," the fact that "partnerships are exponentially powerful" in the cyber domain (e.g. allowing NSA and others to "reach 400 million, 1.5 billion endpoints" and provide them with malware alerts), and the impact of the Intelligence Community being able to release so much information publicly, which "built a coalition, disrupted an adversary, enabled a partner." ([Cyber Collaboration in the Age of Hybrid Warfare: A Conversation With Jen Easterly and Paul Nakasone | Council on Foreign Relations \(cfr.org\)](#))

October 12, 2022 – Taiwan's National Security Bureau Director-General Chen Ming-tong tells Parliament that China has been watching military developments in Ukraine. "This year, the communist military has borrowed from the experience of the Russia-Ukraine war to develop 'hybrid warfare' against Taiwan and strengthen its combat training and preparation against strong enemies." ([Taiwan says China looking at Ukraine war to develop 'hybrid' strategies | Reuters](#))

October 12, 2022 – Lt. Gen. Daniel Karbler, commanding general of U.S. Army Space and Missile Defense Command, tells reporters at the Association of the U.S. Army conference that the Army is gaining lessons from the war in Ukraine about how to move intelligence much more speedily from satellites to ground units, reports Defense One. Lessons include ensuring effective planning so that satellites are

available when needed, and acquiring new software that can provide time and location of targets then use AI to gather data from overhead satellites. “We’re working now on this thing called Skykit, which is, like, basically this software in a Pelican case with a Starlink attached to it. And it’s like, how do you give them a laptop, a Starlink and a ruggedized case so that any unit in their truck can go back and do all this work in a fully offline disconnected fashion? These little autonomous units, how do we empower them?” ([The Ukraine War Is Teaching the US How to Move Intelligence Faster - Defense One](#))

October 13, 2022 – NATO releases an “Autonomy Implementation Plan” which lays out concepts and desired outcomes involving the use of autonomous systems that are “transforming our societies” and “offer clear opportunities [for] bolstering deterrence and defence, preserving NATO’s technological edge,” and other benefits. ([NATO - Official text: Summary of NATO’s Autonomy Implementation Plan, 13-Oct.-2022; War in Ukraine accelerates global drive toward killer robots \(theconversation.com\)](#))

October 14, 2022 – Elon Musk tweets that SpaceX can’t keep funding Starlink services in Ukraine “indefinitely.” He says they are not asking to be paid for past expenses but that it is “unreasonable” to be expected to continue underwriting the service “\*and\* send several thousand more terminals that have data usage up to 100X greater than typical households.” He adds: “We’ve also had to defend against cyberattacks & jamming, which are getting harder.” ([Musk says SpaceX cannot fund Ukraine's vital Starlink internet indefinitely | Reuters](#))

October 14, 2022 – CyberScoop posts an interview with former CrowdStrike CTO Dmitri Alperovitch. Asked if he expects Vladimir Putin to accelerate cyberattacks in the next few months, he responds: “They’re pretty much throwing everything but the kitchen sink at Ukraine already in cyber, but they have been remarkably restrained — surprisingly so — against the West. What you’re seeing now, particularly in the last couple of months, is him slowly escalating vis-a-vis the West and you’ve seen that in his energy policy, shutting down Nord Stream One. If he’s behind the blowing up of the Nord Stream One and Nord Stream Two pipelines, that would be another indication of major escalation. So, you could see him increasingly probe and try to test the West, and cyber could be part of that.”

Commenting on Taiwan’s predicament, Alperovitch draws parallels and differences with Ukraine: “Cyber is always an element of both espionage and warfare as we’re seeing today in Ukraine, as we’ve seen from China for several decades now. It’s not going to be a decisive element of it. Taiwan has a unique vulnerability — it’s an island. Unlike Ukraine, there’s no Poland that is nearby to resupply Taiwan. Virtually all the communications come through undersea cables that could get cut. Some are satellite enabled and could be disrupted through cyberattacks, as we have seen in Ukraine. Imagine a situation where Taiwan is nearly cut off from the outside world. Look at what Ukraine has been able to do by putting out Zelensky videos every night, by having him communicate on virtually every TV channel to rally support for his country. If someone is not able to do that,



it's going to be much more difficult for them to rally the world to their cause.”  
([Dmitri Alperovitch on Taiwan, China and Putin's probing cyberattacks](#)  
([cyberscoop.com](#)))

October 15, 2022 – A few days after CNN reports that SpaceX has asked the Pentagon to assume the costs of providing Starlink services in Ukraine, Elon Musk tweets: “The hell with it ... even though Starlink is still losing money & other companies are getting billions of taxpayer \$, we’ll just keep funding Ukraine govt for free.” However, another CNN report contradicts Musk’s claim to be footing the bill, citing SpaceX correspondence with the Defense Department obtained by the network. CNN writes: “Though Musk has received widespread acclaim and thanks for responding to requests for Starlink service to Ukraine right as the war was starting, in reality, the vast majority of the 20,000 terminals have received full or partial funding from outside sources, including the US government, the UK and Poland, according to the SpaceX letter.”

In the report a senior defense official complains that SpaceX has “the gall to look like heroes” while getting payments from other sources and now reportedly asking for tens of millions more per month. Another CNN story quotes a senior Pentagon official confirming negotiations are ongoing. “Everyone in our building knows we’re going to pay them.” ([\(9\) Elon Musk on Twitter; Ukraine suffered a comms outage when 1,300 SpaceX satellite units went offline over funding issues | CNN Politics](#); [Exclusive: Musk's SpaceX says it can no longer pay for critical satellite services in Ukraine, asks Pentagon to pick up the tab | CNN Politics](#))

October 15, 2022 – Bulgarian Prosecutor General Ivan Geshev tweets: “State institutions are under attack, possibly by Russian hacking groups. The prosecutor’s office, together with the security services, will protect the Bulgarian national interest and that of our European partners from malicious influence.” The pro-Russian hacker Killnet claims responsibility as retaliation for “betrayal to Russia” and delivering arms to Ukraine. ([\(9\) Ivan Geshev on Twitter; Killnet targets Eastern Bloc government sites, but fails to keep them offline - The Record by Recorded Future](#))

October 16, 2022 – *The Hill* posts a story citing various experts who worry that Vladimir Putin may intensify Russia-backed cyberattacks during the November U.S. midterm elections. ([Ongoing US support to Ukraine could prompt Russian cyber escalation in midterms, experts warn | The Hill](#))

October 16-17, 2022 – Secretary of State Antony Blinken, along with Ambassador at Large for Cyberspace and Digital Policy Nate Fick and Assistant Secretary for Economic and Business Affairs Ramin Toloui, travel to the San Francisco area to meet with academics and private sector companies to spotlight “the key role for technology diplomacy in advancing U.S. economic and national security,” according to the State Department. Media reports indicate that deep concerns about the threat of cyberwar are on the administration’s agenda. ([Secretary Blinken’s Travel to California, October 16-17 - United States Department of State](#); [Antony Blinken’s](#)

[Silicon Valley visit underscores US cybersecurity concerns | Cyberwar | The Guardian](#))

October 17, 2022 – Russian-launched “kamikaze” drones hit Kyiv, killing at least eight people. ([Ukraine war: Russia dive-bombs Kyiv with 'kamikaze' drones - BBC News](#))

October 17, 2022 – A Czech disinformation expert affiliated with an organization established by the European Union and NATO tells Radio Free Europe the West is unwittingly helping Vladimir Putin by buying into worst-case fears of what he might do. Jakub Kalensky of the European Center of Excellence for Countering Hybrid Threats, based in Helsinki, tells the outlet: “As a disinformation or propaganda specialist, what I see is 15 years of empty threats being used over and over and over again [by Moscow] simply because they are paralyzing us. So all I'm saying is that we shouldn't fall for this trap, because that only helps Putin to achieve his goal, and it harms Ukrainians who are actually fighting for our European or Euro-Atlantic values.” ([‘It's Time To Ignore' The Traps: Disinformation Expert Says Kremlin's 'Empty Threats' Have Paralyzed The West \(ampproject.org\)](#))

October 18, 2022 – German Interior Minister Nancy Faeser releases the head of the country's national cyber security agency from his duties after media reports that he has ties to Russian intelligence. The reports link Arne Schönbohm, president of the Federal Office for Information Security (BSI) since 2016, to an entity called the German Cyber Security Council, one of whose member companies was reportedly founded by a former Russian intelligence agent. The Interior Ministry says that an investigation will commence and until then “the presumption of innocence applies to Mr. Schönbohm.” ([Subscribe to read | Financial Times \(ft.com\)](#); [BSI - Management \(bund.de\)](#))

October 18, 2022 – Estonian Defense Minister Hanno Pevkur visits the Pentagon for bilateral talks. ([Estonia's defense minister on Ukrainian lessons, future investments and Russia's cyber threat - Breaking Defense](#))

October 19, 2022 – Ukrenergo, the country's national energy company, calls on Ukrainians to “charge everything” by the following morning in anticipation of power cuts from Russian missile attacks. ([Ukrainians told to 'charge everything' as power grid hit by Russia - BBC News](#))

October 19, 2022 – Viktor Zhora, deputy chairman and chief digital transformation officer at Ukraine's SSSCIP, tells attendees at Mandiant's Worldwide Information Security Exchange event in Washington that despite the huge rise in Russian cyberattacks starting in February, “the adversary hasn't reached its strategic goals in the cyber war against Ukraine.” ([Russia Failing to Reach Cyber War Goals, Ukrainian Official Says – MeriTalk](#))

October 19, 2022 – The following appears on the website of Alexander Khinshtein, a Russian Duma member: “Chair of the State Duma committee on information policy

Alexander Khinshtein declared that Russia must open an IT front and called for cyber strikes against Ukraine. The deputy discussed the topic of cyber warfare on his Telegram channel.” The posting somewhat mystifyingly goes on to urge that “Russia must move from defense to attack.” (Risky Biz News, 10-21-2022; [Глава комитета Госдумы Хинштейн призвал к киберударам по центрам принятия решений Украины | Александр Хинштейн \(hinshtein.ru\)](#))

October 19, 2022 – Rob Joyce, director of the NSA Cybersecurity Directorate, tells the Trello Cybersecurity Summit in Washington that intelligence sharing on cyberthreats “can really make a big and decisive difference.” He says this is a key lesson NSA “took away personally” from the war in Ukraine. “Over time, I’ve changed my view about what it is to protect sources and methods,” he says. “[W]hat we know is often not sensitive, it is how we know it ... We can make available the insights about what we know without putting at risk how we know it. That’s really an inflection point that lets us get to more prolific, more extensive and more closely sharing for operational outcomes.” He says there have been 8,500 “analytic exchanges” through the the agency’s Cybersecurity Collaboration Center this year involving private industry. ([NSA cyber chief says Ukraine war is compelling more intelligence sharing with industry \(cyberscoop.com\)](#))

October 19, 2022 – A hotel converted to host Ukrainian refugees in Gross Strömkendorf in northeastern Germany burns down. Not long afterwards a video appears on YouTube with the logo of *Bild*, a German tabloid, and bearing a chyron claiming Ukrainian refugees started the blaze. In fact, German authorities later identify a 32-year-old German serial arsonist with no apparent political motivation as the culprit. The video soon spreads to numerous other social media platforms leading the *Washington Post* to include it as an example of Moscow’s latest disinformation tactic – creating rifts and distrust between European host countries and the Ukrainian evacuees they are sheltering. ([Russian disinformation aims to turn Germany against Ukrainian refugees - The Washington Post](#); [Germany: Suspect arrested after fire in refugee accommodation - InfoMigrants](#))

October 20, 2022 – The IT Army of Ukraine hits Russia’s Federal Tax Service with a DDoS attack preventing Russian citizens from submitting their taxes or retrieving documents. Two days later, the group repeats the attack. ([Development of the Ukrainian Cyber Counter-Offensive | Trustwave](#))

October 20, 2022 – European Union member states vote to freeze the assets of three individuals and one entity relating to Iran’s supply of drones to Russia. Four other Iranian entities already under sanction may face additional measures. ([EU agrees on new Iran sanctions over drone deliveries to Russia -EU presidency | Reuters](#))

October 20, 2022 – Ukraine’s Security Service announces it has taken down another Russian bot farm, this one running some 10,000 fake accounts. It is reported to be the sixth such operation since February. (Risky Biz News, 10-21-2022; [The SSU](#)

[liquidated an enemy bot farm in Dnipro, which created almost 10 thousand hectares. fake accounts to "disperse" Kremlin propaganda in the EU\)](#)

October 20, 2022 – A Ukrainian official tells KAN news that 10 Iranian military advisers training Russian soldiers in occupied Ukrainian territory have been killed over the past week. Ukraine alleges that Iranian instructors are in Kherson and Crimea where they are teaching Russian forces how to use Shahed-136 kamikaze drones and then monitoring operations. ([10 Iranians killed in Ukrainian strikes - report - The Jerusalem Post \(jpost.com\)](#))

A month later, Oleksiy Danilov, secretary of Ukraine's national security and defense council, confirms Iranians have been in Crimea and that some have been killed. "You shouldn't be where you shouldn't be," he says in an interview in Kyiv. "They were on our territory. We didn't invite them here, and if they collaborate with terrorists and participate in the destruction of our nation we must kill them." ([Iranian advisers killed aiding Russians in Crimea, says Kyiv | Ukraine | The Guardian](#))

October 20, 2022 – Speaking at a CyberScoop CyberTalks event, Col. Candice Frost, commander of U.S. Cyber Command's Joint Intelligence Operations Center, discusses the development of partnerships with the NSA, FBI, CISA, and other federal agencies during the course of the war in Ukraine. "It's been phenomenal to see this. In my intelligence background, and in what I've done for almost 25 years, I've never seen this sharing between agencies and also writ large with the American public – and I find that partnership is so important, especially in cybersecurity," Frost says. ([Cybercom exec calls for deeper threat intel-sharing as warfare evolves \(defensescoop.com\)](#))

October 21, 2022 – CERT-UA begins to detect a series of phishing emails impersonating the Press Service of Ukraine's General Staff. The agency shortly afterwards posts an alert about possible Cuba Ransomware attacks. ([Cuba ransomware affiliate targets Ukrainian govt agencies \(bleepingcomputer.com\)](#))

October 21, 2022 – *Lawfare* posts an analysis of Killnet, concluding "Killnet's primary impact is not its unsophisticated cyberattacks but its ability to shape the cognitive environment and the narratives surrounding the war—both for its followers on Telegram and among the Western media." ([What Impact, if Any, Does Killnet Have? - Lawfare \(lawfareblog.com\)](#))

October 22, 2022 – *The Record* publishes an interview with Kenneth Geers, a visiting academic in Ukraine from 2014-2017 and currently an analyst at the company Very Good Security. Addressing lessons from the war in Ukraine, Geers comments that "the defense has seemed to play a bigger role than the offense. We see that Ukrainian cyber defense has matured over the years, which is probably why it's more difficult for Russian hackers to achieve significant damage in Ukraine. Russia, in turn, is known for its offensive operations but cares little about cyber defense. Russian computer systems often use old unpatched software and are therefore very



vulnerable to malware attacks. Foreign hackers supporting Ukraine now have a field day in Russia. Because of the war, they feel they have the moral and ethical right to hack into Russia. And there's plenty of space to hide in Russian networks – they are so bad.” ([Q&A: Kenneth Geers on the cyber war between Ukraine and Russia - The Record by Recorded Future](#))

October 23, 2022 – A one-time leader of the JabberZeus Crew, a Ukrainian national named Vyacheslav Igorevich Penchukov, is arrested in Geneva. A federal grand jury in Nebraska first indicted him and two associates in 2012 on an array of charges stemming from their use of the malicious software “Zeus” to steal millions from mostly small and medium-sized businesses. ([JABBERZEUS SUBJECTS — FBI; Top Zeus Botnet Suspect “Tank” Arrested in Geneva – Krebs on Security](#))

October 24, 2022 – Some 1,300 Starlink terminals go offline, causing a “huge problem” for Ukraine’s military, a source tells CNN; the source adds that the outage occurred because of a lack of funding. ([Ukraine suffered a comms outage when 1,300 SpaceX satellite units went offline over funding issues | CNN Politics](#))

October 24, 2022 – A Bellingcat employee tweets: “New on @bellingcat: we (mostly @christogrozev) identified the team of Russian programmers who guide the rockets attacking Ukraine. Christo even identified who was working on which missile type.” The most recent attacks took place on October 10-11 and continued into the following week. ([\(10\) Aric Toler on Twitter](#))

A lengthy report by Bellingcat today describes the results of a six-month investigation, conducted with the *Insider* and *Der Spiegel*, into Russian missile attacks. The probe relied on open-source intelligence and leaks of Russian information. “Phone metadata shows contacts between these individuals and their superiors spiked shortly before many of the high-precision Russian cruise missile strikes that have killed hundreds and deprived millions in Ukraine of access to electricity and heating. The group, which works from two locations – one at the Ministry of Defence headquarters in Moscow and another at the Admiralty headquarters in St. Petersburg – is buried deep within the Russian Armed Forces’ vast “Main Computation Centre of the General Staff”, often abbreviated as ГВЦ (GVC).

Describing its methodology, Bellingcat continues: “The identification of this clandestine group within the Ministry of Defence was made by parsing through open-source data of thousands of graduates of Russia’s leading military institutes that focus on missile engineering and programming .... Bellingcat analysed leaked employment or telephone entry data on these graduates available via Russia’s underground data markets. This allowed us to discover that some of these people were referenced in phone contact lists, obtained from various data lookup Telegram bots such as Glaz Boga and HimeraSearch, as working at GVC (Главный Вычислительный Центр) or the Main Computation Centre of the Armed Forces of Russia. Notably, all of these military missile engineering graduates with a GVC reference linked to their phone numbers in these apps were registered as living and working at Znamenka Street 19 in Moscow — the official address of Russia’s Armed

Forces General Staff.” ([The Remote Control Killers Behind Russia’s Cruise Missile Strikes on Ukraine - bellingscat](#))

October 24-28, 2022 – During its annual conference in Belgrade, the Réseaux IP Européens (RIPE), the organization that manages IP addresses in Europe, agrees to enact a “temporary freeze” on transfers of Ukrainian IP addresses, particularly to Russian entities. Ukrainian members of the group pleaded for action, recounting incidents of forced transfers “at gun point.” ([RIPE meetings: IP addresses as spoils of war – TechAint](#); [Risky Biz News: OPERA1ER group hits African banks for \\$30 million \(substack.com\)](#))

October 25, 2022 – Germany’s BSI releases its annual report on the state of IT in Germany. This year it notes “an accumulation of minor incidents and hacktivism campaigns in Germany in connection with Russia’s war of aggression against Ukraine” but reports that a “comprehensive attack campaign against German targets was not apparent.” It concludes that threats emanating from ransomware and political hacks are “higher than ever.” ([German cyber agency warns threat situation is ‘higher than ever’ - The Record by Recorded Future](#); [BSI - Die Lage der IT-Sicherheit in Deutschland \(bund.de\)](#))

October 25, 2022 – Bloomberg reports quotes senior Ukrainian cyber official Victor Zhora as saying the Ukrainian government is preparing to share evidence of Russian hacking activity with the International Criminal Court. Zhora adds this would be “the first prosecution of the first global cyber-war.” ([The Cipher Daily Brief for Wednesday, October 26, 2022 \(mailchi.mp\)](#); [Ukraine Documenting Russian Hacks, Eyeing International Charges - Bloomberg](#))

October 25, 2022 – The U.S. Attorney’s Office for the Western District of Texas posts a press release advising: “A newly unsealed federal grand jury indictment charges Mark Sokolovsky, 26, a Ukrainian national, for his alleged role in an international cybercrime operation known as Raccoon Infostealer, which infected millions of computers around the world with malware.” Sokolovsky is currently in custody in the Netherlands pursuant to a U.S. extradition request. A separate account reports that he was apprehended in March after trying to evade mandatory military service in Ukraine. Yet another report indicates he fled Ukraine with his girlfriend who “documented everything on Instagram.” ([Newly Unsealed Indictment Charges Ukrainian National with International Cybercrime Operation | USAO-WDTX | Department of Justice](#); [Accused ‘Raccoon’ Malware Developer Fled Ukraine After Russian Invasion - Krebs on Security](#); [\(10\) vx-underground on Twitter](#))

October 25, 2022 – Former *Washington Post* reporter Walter Pincus writes that the conflict in Ukraine presents a window onto the future of war. “Like the 1936–1939 Spanish Civil War, Russia’s invasion of Ukraine has created a testing ground for the next generation of tactics and weapons to be employed by major powers in future fighting.” These include the Switchblade 300 kamikaze drone. The article appears in

*The Cipher Brief.* ([In Ukraine, We're Witnessing the Future of War \(thecipherbrief.com\)](https://thecipherbrief.com))

October 25, 2022 – Recorded Future's Insikt Group identifies a threat group called BlueBravo which it says tried to use a fictitious ambassador's schedule as part of a lure operation. An earlier report about a similar attempt related to the Embassy of Israel. BlueBravo "overlaps with the Russian advanced persistent threat (APT) activity tracked as APT29 and NOBELIUM. APT29 and NOBELIUM operations have been previously attributed to Russia's Foreign Intelligence Service (SVR)." ([BlueBravo Uses Ambassador Lure to Deploy GraphicalNeutrino Malware \(recordedfuture.com\)](https://recordedfuture.com))

October 26, 2022 – Ukraine's Victor Zhora tells the 2022 Blackberry Security Summit that after "a huge growth within the first months of war and a number of highly sophisticated attacks in March and April," the Ukrainians currently "see no particular strategy, and we see rather opportunistic behavior" on Russia's part. ([Ukraine: Russian cyber attacks aimless and opportunistic \(techtarget.com\)](https://techtarget.com))

October 26, 2022 – A tweet tied to a fictitious account and soliciting donations for Ukraine is identified by Domain Tools as part of its investigation into a cryptocurrency scam involving impersonation of the country's Ministry of Digital Transformation. Domain Tools posts a lengthy report a few weeks later (December 8). ([Crypto Winter: Fraudsters Impersonate Ukraine's Government to Steal NFTs and Cryptocurrency - DomainTools | Start Here. Know Now.](https://cryptowinter.com))

October 27, 2022 – Foreign Minister Dmytro Kuleba says Ukrainian forces have shot down 260 Iranian-made drones Russia has been deploying in Ukraine. "They're not as good as one might think," he reports, "and the number of drones that we have shot down speaks for itself. But they still inflict a lot of damage." He adds that Ukraine first got word of Iran's plans to supply drones to Russia several months ago. Iran gave verbal and written assurances it would not happen, he says. ([Ukraine says it has shot down over 250 Iranian-made drones used by Russia \(axios.com\)](https://axios.com))

October 27, 2022 – The Slovak and Polish parliaments are hit by cyberattacks, according to officials in both countries. "The attack was multi-directional," a Polish Senate statement reads, "including from inside the Russian Federation." Polish Senate speaker Tomasz Grodzki speculates it is tied to a Senate vote the day before that labeled the Russian government a "terrorist regime." Slovak deputy speaker of parliament Gabor Grendel tells AFP: "Parliament's entire computer network has been paralyzed." ([Slovak, Polish Parliaments Hit By Cyber Attacks | Barron's \(barrons.com\)](https://barrons.com))

October 27, 2022 – Mondelez International and Zurich American Insurance Co. settle a \$100 million lawsuit over the latter's denial to cover a claim resulting from the 2017 NotPetya attack. Mondelez had argued that the "act of war" exception should not apply because the impact was "collateral damage" in a larger cyber conflict that had

nothing to do with the company. The settlement is said to be likely to have a huge impact on the cyber insurance marketplace. ([Mondelez, Zurich Settle NotPettya Dispute Before Trial Close - Law360](#); [Insurance giant settles NotPettya lawsuit, signaling cyber insurance shakeup \(cyberscoop.com\)](#))

October 27, 2022 – (Date approx.) Konstantin Vorontsov, deputy director of the Russian Foreign Ministry's department for non-proliferation and arms control, tells the United Nations First Committee that the West is using satellites to enforce its dominance over other regions, calling it “an extremely dangerous trend.” He continues: “Quasi-civilian infrastructure may be a legitimate target for a retaliatory strike.” ([Russia warns West: We can target your commercial satellites | Reuters](#))

October 27, 2022 – On or about this date, Ukrainian officials unveil the “Delta situational awareness system” during NATO’s biannual TIDE Sprint conference. “According to a Ukrainian military statement, “Delta provides a comprehensive understanding of the battle space in real time. It also integrates information about the enemy from various sensors and sources, including those from intelligence, on a digital map. The Delta doesn’t require any additional settings and can work on any device: on a laptop, tablet or mobile phone.” Delta software is being developed by the Defense Technology Innovation and Development Center of the Ukrainian Ministry of Defense with the support of the Ministry of Digital Transformation and unnamed foreign allies. ([Ukraine unveiled its own Delta situational awareness system - Militarnyi](#))

October 28, 2022 – The JailBreak Security Summit (“The world's only security summit held at a production brewery”) features several speakers discussing Ukraine- and Russia-related cyber activities. Margin Research’s Justin Sherman, for example, presents on “Russia’s Open-Source Code and Private-Sector Cybersecurity Ecosystem,” a talk that focuses on DARPA’s SocialCyber project which examines that ecosystem and the threats it faces. (Video: [Justin Sherman: Russia's Open-Source Code and Private-Sector Cybersecurity Ecosystem on Vimeo](#); conference site: [Jailbreak Brewing Company Security Summit \(jailbreaksecuritysummit.com\)](#); article by Sherman: [Russia's Open-Source Code and Private-Sector Cybersecurity Ecosystem — Margin Research](#))

October 29, 2022 – Seven maritime drones (“unscrewed surface vessels” – USVs) penetrate the Russian-controlled port of Sevastopol. Although they only cause minor damage to two vessels, the event is later deemed a “turning point in naval history,” by one private news outlet. “This is not the first time that explosive laden USVs have been used to attack enemy ships in conflict,” writes *Naval News*. “But it is the clearest and cleanest example to date, and the maritime drones involved more closely match modern technologies. These drones leveraged modern communication systems (likely Starlink), and mass tactics. The number involved and degree of coordination was short of ‘swarm tactics’, but it was halfway there. So it may be a preview of wars to come.” Furthermore, “The drones were small and relatively cheap. Despite using the latest technology, they were the sort of thing which can be built in almost any



garage. They leverage off-the-shelf civilian components such as popular jet skis.”  
([Why Ukraine’s Remarkable Attack On Sevastopol Will Go Down In History - Naval News](#))

October 30, 2022 – The BBC publishes an article describing USCYBERCOM’s hunt forward operations related to Ukraine. Clearly approved by the U.S. government, the article features quotes from senior officers and operatives from some of the missions.  
([Inside a US military cyber team’s defence of Ukraine - BBC News](#))

October 31, 2022 – Russian forces undertake missile and drone attacks on 18 targets in 10 regions across Ukraine, according to Prime Minister Denys Shymal. (Interestingly, cyber attacks are not immediately reported to be part of the assault.) ([Russia-Ukraine war live updates: Power out in Kyiv, key cities after energy strikes - The Washington Post](#))

October 31, 2022 – The White House convenes the Second International Counter Ransomware Initiative (CRI) Summit October 31-November 1, 2022. Representatives of 36 countries and the EU attend. “Throughout the Summit, CRI and private sector partners discussed and developed concrete, cooperative actions to counter the spread and impact of ransomware around the globe,” a White House fact sheet reports. ([FACT SHEET: The Second International Counter Ransomware Initiative Summit | The White House](#))

October 31, 2022 – According to a later Reuters special report, “At least \$2.6 billion of computer and other electronic components flowed into Russia in the seven months to Oct. 31, Russian customs records show. At least \$777 million of these products were made by Western firms whose chips have been found in Russian weapons systems: America’s Intel Corp, Advanced Micro Devices Inc (AMD), Texas Instruments Inc and Analog Devices Inc., and Germany’s Infineon AG.” ([The supply chain that keeps tech flowing to Russia \(reuters.com\)](#))

October 31, 2022 – *The Record* publishes an interview with the deputy manager of Latvia’s CERT in which he describes the range of attacks his country has encountered from pro-Kremlin hacktivists such as Killnet, XakNet and FuckNet. He says their collective impact has been unimpressive. “Russian hacktivists are a PR project, not talented hackers,” he says. Of greater concern are possible attacks by APT groups. To counter these threats, Latvia has two CERTs – one focusing more on government systems and critical infrastructure, the other on military networks. ([Latvia’s cyberspace faces new challenges amid war in Ukraine - The Record by Recorded Future](#))

October 31, 2022 – Radio Free Europe posts an article about a day in the life of a drone operator in Ukraine’s military. It notes that hundreds of drone operators are being trained every month and a large cohort of volunteers are constantly raising funds to buy more units. The article goes on to describe the daily routine of a drone pilot: “On a typical flight day, they’ll fly their camera-equipped drone over Russian positions,

bring it back to their lines, and return to their base to upload their flight camera's data into their computers. The team then begins the painstaking process of identifying the location of Russian vehicles and bases. In order to find Russia's often well-camouflaged equipment in their footage, they first use artificial intelligence to identify square objects. They then pore over the footage for hours, examining it closely for signs of targets.” ([Near The Front, Ukraine's Drone Pilots Wage A Modern War On A Shoestring Budget \(rferl.org\)](#))

November 2022 – Aurélio Blanquet, secretary general of the European Energy Information Sharing and Analysis Center, tells a conference in Brussels that based on recent cyberattacks in 2022, “We can talk about a weaponization of the energy sector.” ([European Electricity Sector Lacks Cyber Experts as Ukraine War Raises Hacking Risks \(wsj.com\)](#))

November 2022 – ESET detects new ransomware in Ukraine that it calls RansomBoggs and attributes to Sandworm. “The ransomware has multiple references to Monsters, Inc. We observed that malware operators used POWERGAP scripts to deploy this file coder.” ([eset apt activity report t32022.pdf \(welivesecurity.com\)](#))

Early November 2022 – Tehran and Moscow strike a deal to build large numbers of weaponized drones inside Russia, according to unnamed officials from two countries monitoring the negotiations who are cited in a later report by the *Washington Post*. ([Iran will help Russia build drones for Ukraine war, officials say - The Washington Post](#))

November 1, 2022 – A Russian court fines the Wikipedia Foundation 2 million roubles (\$32,600) for not deleting items about the Ukraine war as demanded by Russia, according to Stanislav Kozlovsky, head of the foundation's Russia chapter. He indicated the foundation would appeal. ([Russia fines Wikimedia Foundation over Ukraine war entries | Reuters](#))

November 1, 2022 – The British Foreign Office provides first-ever confirmation that GCHQ has been helping Ukraine with cyber defense assistance. Announcing the annual review of the National Cyber Security Centre (NCSC), Foreign Secretary James Cleverly comments that Britain has been utilizing its “world-leading expertise to support Ukraine’s cyber defenses. Together, we will ensure that the Kremlin is defeated in every sphere: on land, in the air and in cyber space.” ([UK boosts Ukraine's cyber defences with £6 million support package - GOV.UK \(www.gov.uk\)](#); [UK government confirms its intel agency is helping to defend Ukraine - The Record by Recorded Future](#))

A BBC report today provides more information, based mostly on unnamed sources. Among other details is that the U.K. so far has spent £6 million defending Ukraine in cyberspace. One named source, Leo Docherty, Europe minister at the Foreign Commonwealth and Development Office (FCDO), tells the outlet: “We brought some of our expertise to bear on helping them defend from what has been a daily onslaught of cyberattacks from Russia since the start of the invasion.” The

article adds that the FCDO has been the agency providing the support, “with officials saying it has led the way amongst allies in providing specialist expertise.” ([Ukraine War: UK reveals £6m package for cyber defence - BBC News](#))

November 1, 2022 – The pro-Russian hacktivist group Joker DPR claims to have breached the Ukrainian battlefield management system Delta, an assertion the country’s Ministry of Defense denies and Recorded Future says later is “unlikely to be completely true.”

November 2, 2022 – Blackberry reports that a threat actor called RomCom is running a series of attacks exploiting SolarWinds, KeePass, and PDF Technologies. The BlackBerry Threat Research and Intelligence Team discovered the activity while investigating a previously known threat actor, RomCom RAT, which was targeting Ukrainian military entities. “While Ukraine still appears to be the primary target of this campaign, we believe some English-speaking countries are being targeted as well, including the United Kingdom .... Given the geography of the targets and the current geopolitical situation, it's unlikely that the RomCom RAT threat actor is cybercrime-motivated.” ([RomCom Threat Actor Abuses KeePass and SolarWinds to Target Ukraine and Potentially the United Kingdom \(blackberry.com\)](#))

November 3, 2022 – Mykhailo Federov, head of Ukraine's digital transformation ministry, tells a news conference that he trusts Elon Musk to continue supporting Ukraine’s access to Starlink services. “[W]e had a conversation with him about it, so we do not see a problem in this regard.” However, he adds that Ukraine will also be seeking additional providers. ([Ukraine trusts Musk's Starlink but looking for other providers too | Reuters](#))

November 3, 2022 – Microsoft’s Brad Smith pledges more than \$100 million in additional aid to Ukraine’s “extraordinary” effort to counter the Russian invasion. The financial assistance will extend to the end of 2023, Smith tells the annual Web Summit conference in Lisbon, and will bring Microsoft’s total support to Ukraine since February to \$400 million. (Notably, Smith is accompanied at the announcement by Ukraine’s Mhkhailo Fedorov, who the same day is reported to be seeking providers of communications systems other than Starlink – see entry above.) ([Microsoft extends aid for Ukraine’s wartime tech innovation \(c4isrnet.com\)](#))

November 3, 2022 – IT Army hackers break into Russia’s Central Bank, releasing 27,000 files on the bank’s operations, security policies, and other information. A data security analyst calls it a “treasure trove with insights and stories that could have catastrophic consequences for Russia.” Bank officials pooh-pooh the incident, claiming “not a single information system of the Bank of Russia has been hacked.” ([Ukrainian hacktivists claim to leak trove of documents from Russia’s central bank - The Record by Recorded Future](#); The CyberWire, 11-8-2022)

November 3, 2022 – The European Union Agency for cybersecurity (ENISA) releases its 10<sup>th</sup> Threat Landscape report, identifying threats, trends, and mitigation measures. The 150-page report notes: “The Russia-Ukraine crisis has defined a new era for cyberwarfare and hacktivism, its role, and its impact on conflicts. States and other cyber operations will very likely adapt to this new state of affairs and take advantage of the novelties and challenges brought about by this war. However, this new paradigm brought by the war has implications for international norms in cyberspace and, more specifically, for state sponsorship of cyberattacks and against targeting critical civilian infrastructure. Due to the volatile international situation, we expect to observe more cyber operations being driven by geopolitics in the near to mid-term future. The geopolitical situation might trigger cyber operations and potentially damaging cyberattacks. Consequently, a destabilized situation and continued threshold exceedance in terms of malicious cyber activity may also lead to more resulting damage.” (“ENISA Threat Landscape 2022”)

November 3, 2022 – The Carnegie Endowment for International Peace puts out a report, “Evaluating the International Support to Ukrainian Cyber Defense.” Focusing on the defense of Ukraine’s digital networks, the report draws on interviews with private sector experts as well as Ukrainian government sources. Author Nick Beecroft also offers five lessons gleaned so far. ([Evaluating the International Support to Ukrainian Cyber Defense - Carnegie Endowment for International Peace](#))

November 4, 2022 – The FBI puts out a Private Industry Notification on hacktivism intended to ask organizations to take recommended steps to minimize the impact of any attacks. The posting includes the comment: “Coinciding with the Russian invasion of Ukraine, the FBI is aware of Pro-Russian hacktivist groups employing DDoS attacks to target critical infrastructure companies with limited success.” The notice adds that these “generally opportunistic attacks” tend to have “minimal operational impact” but the perpetrators “will often publicize and exaggerate the severity of these attacks on social media.” ([221104.pdf \(ic3.gov\)](#))

November 4, 2022 – The Defense Department announces it will provide additional drones to Ukraine. In addition to 700 Switchblade “one-way” unmanned aerial systems (UAS) already committed, the U.S. will send 1,100 Phoenix Ghost systems, or kamikaze drones, as part of a new \$400 million security assistance package announced Friday. DefenseScoop reports that DOD will buy the Phoenix Ghosts from industry with Ukraine Security Assistance Initiative (USAI) funds, a process that generally takes longer than using presidential drawdown authority to take them from DOD stocks. ([US more than doubling its commitment of Phoenix Ghost kamikaze drones to Ukraine \(defensescoop.com\)](#))

November 4, 2022 – “Microsoft Digital Defense Report 2022” is published. The 114-page report is replete with references to all aspects of cyber activity and lessons connected to the war in Ukraine, which it characterizes as “the dawn of a new age of conflict.” ([Microsoft Digital Defense Report 2022](#))



November 5-6, 2022 – Killnet attempts several DDoS attacks against the websites of state intelligence agencies in Estonia, Poland, Romania, Bulgaria, and Moldova. The impact is reportedly brief and insignificant. Cybersecurity experts tell *The Record* that Killnet’s level of sophistication is relatively low and that media accounts tend to blow up its impact. ([Killnet targets Eastern Bloc government sites, but fails to keep them offline - The Record by Recorded Future](#))

November 7, 2022 – Gen. Sir Jim Hockenham, commander of the U.K.’s Strategic Command, delivers a lengthy assessment to the Royal United Services Institute concerning new developments in types and usage of open source intelligence (OSINT) growing out of the war in Ukraine. ([How open-source intelligence has shaped the Russia-Ukraine war - GOV.UK \(www.gov.uk\)](#))

November 7, 2022 – *Breaking Defense* publishes an October interview with Estonian Defense Minister Hanno Pevkur on the lessons of the war in Ukraine. Opening with a comment on Russia’s general conventional approach to combat, he remarks: “First lesson is that the strategy, or mostly the tactics, from the Russian army hasn’t changed since the Second World War.” Asked if Russia’s cyber capabilities have been exaggerated, he replies: “The threat is still there, and the capabilities are still there. So this is something you know that — I always say that with cyber attacks, it can cause more problems for societies, for civil societies, [than with] conventional attacks. Because with a cyber attack, you can basically take down the electricity or the energy supply for the whole of Kyiv. With the bombing you can take down maybe a part of the city. So in that sense, the cyber threat is something we cannot avoid and we have to be ready for that. But I also believe that in tackling the cyber threats, it is very, very crucial and very, very important to make a good cooperation with the civil forces, with the private contractors. And of course, I also believe that every infrastructure company has to be ready to tackle all kinds of cyber threats. Because it’s just unimaginable what you can do with the cyberattack.” ([Estonia's defense minister on Ukrainian lessons, future investments and Russia's cyber threat - Breaking Defense](#))

November 7, 2022 – Putin ally and Wagner Group head Yevgenii Prigozhin, tells Russian journalists he is interfering in the U.S. midterm elections. Months later, he admits that he founded the Internet Research Agency, something the Treasury Department long ago concluded. ([Yevgeniy Prigozhin, Putin ally, boasts he ‘interfered’ in U.S. elections - The Washington Post](#); [Wagner mercenary chief says he is also behind Russian information war - The Washington Post](#))

November 9, 2022 – Ukraine’s SSSCIP posts a warning: “The experts of the Computer Emergency Response Team of Ukraine CERT-UA detect mass emails containing malicious links allegedly on behalf of the State Service of Special Communications and Information Protection of Ukraine. This activity is attributed to the UAC-0010 group (Armageddon) .... The CERT-UA emphasizes that the emails are being spread using the @mail.gov.ua service. It means that the criminals are getting increasingly scrupulous in disguising themselves as Ukrainian public officials.” The notice

continues: “The UAC-0010 (Armageddon) hacking group is associated with Russia’s Federal Security Service (FSB). They are among the most active groups that have been attacking Ukraine since the beginning of Russia’s full-scale military invasion of Ukraine. Criminals are usually exploiting topics that are sensitive and important for Ukrainians.” ([State Service of Special Communications and Information Protection of Ukraine \(cip.gov.ua\)](https://cip.gov.ua/))

November 9, 2022 – France releases an “intermediate version” of its planning document “National Strategic Review 2022.” The opening section assessing the strategic environment begins: “Russia’s invasion of Ukraine on 24 February 2022 represents a strategic shift. On the one hand, combined with other structural developments, it confirms the observation of changes in the threat assessment described in the 2017 national defence and security strategic with you, updated in 2021. On the other, it calls for an adaptation of our strategic response to build up our moral strength and resilience, consolidate our alliances and accelerate the modernisation of our defence mechanisms.”

Among other notable statements, the document dismisses the utility of cyber deterrence: “There is no way to envisage a cyber shield that would thwart any cyber-attack on France, but strengthening its level of cyber security is essential to prepare the country for more cyber threats. Similarly, the application of a deterrent approach in cyberspace that would force any attacker to restrain himself against France is illusory.” The answer, it continues, is to improve cyber resilience and to “mobilise all the levers of the State, both European and international ... to make cyberattacks particularly costly for the attackers.” ([national-strategic-review-intermediate-version-1.pdf \(sgdsn.gouv.fr\)](https://sgdsn.gouv.fr/national-strategic-review-intermediate-version-1.pdf))

November 9, 2022 – Switzerland releases a provisional version of its annual threat assessment report, which includes the following discussion of the cyber component (slightly modified Google translation):

“In the cyber domain, the main threat to critical infrastructures comes from criminal groups, as evidenced by the sharp increase in the number of attacks perpetrated by means of ransomware in Switzerland and abroad. The tools necessary for such acts can be acquired from specialized criminal suppliers. There is a competitive market in this area of suppliers who, subject to pressure on prices, sometimes go so far as to openly promote their offer.

“While most of the observed cyberattacks are launched for financial reasons, other motives should not be excluded. Violent extremism, terrorism, intelligence activities or power politics can also cause it. Pursuing objectives of another nature, the perpetrators of these acts can go as far as sabotage.

“So far, the war in Ukraine has confirmed that in the context of armed conflicts, cyber means are above all used in a support function. They aim to reduce the adversary’s military capabilities and damage critical infrastructure. Given international interdependencies, such cyberattacks can also cause collateral damage and therefore indirectly affect Swiss facilities.

“Threats to critical infrastructure do not only come from cyber means: physical attacks are also possible for similar motives. Moreover, any conventional

war between industrialized countries threatens a multitude of critical infrastructures and can have direct repercussions on Switzerland, as illustrated by the case of the Zaporizhia nuclear power plant in Ukraine.” ([73756.pdf \(admin.ch\)](#))

November 9, 2022 – The *Financial Times* posits some lessons of the Ukraine experience. Among other experts, the paper quotes Yurii Shchychol, head of Ukraine’s cybersecurity agency: “The key elements of [Ukraine’s] cyber [defense] are: sufficient funding at the national level [and] at private companies managing critical infrastructure; cyber hygiene at all levels; and extensive international cooperation.” He adds that “threat indicators” and joint training exercises are “the two primary aspects of the collective cyber security system.” ([What Ukraine’s cyber defence tactics can teach other nations | Financial Times \(ft.com\)](#))

November 10, 2022 – The “NATO Cyber Defense Pledge Conference 2022” takes place in Rome. Anne Neuberger, deputy national security adviser for cyber and emerging technologies at the White House and Nate Fick, ambassador at large for cyberspace and digital diplomacy, attend. Among other comments, Neuberger notes that “Ukraine has in many cases been able to successfully defend against sophisticated cyberattacks due to the work that was done before the Russian invasion.” ([White House cyber official advocates nimbler NATO to confront digital threats \(cyberscoop.com\)](#))

November 10, 2022 – Mandiant experts at the CyberwarCon security conference present findings concerning the GRU based on months of incident response activity in Ukraine. They say the Russian military intelligence agency has moved away from routine phishing operations toward a practice of targeting “edge” devices such as firewalls, routers, and email servers. “That shift,” as described by *Wired*, “has offered multiple advantages to the GRU. It’s allowed the Russian military hackers to have far faster, more immediate effects, sometimes penetrating a target network, spreading their access to other machines on the network, and deploying data-destroying wiper malware just weeks later, compared to months in earlier operations. In some cases, it’s enabled the hackers to penetrate the same small group of Ukrainian targets multiple times in quick succession for both wiper attacks and cyberespionage. And because the edge devices that give the GRU their footholds inside these networks aren’t necessarily wiped in the agency’s cyberattacks, hacking them has sometimes allowed the GRU to keep their access to a victim network even after carrying out a data-destroying operation.” ([Russia’s New Cyberwarfare in Ukraine Is Fast, Dirty, and Relentless | WIRED](#))

November 10, 2022 – Microsoft updates its blog, concluding that the threat actor IRIDIUM (described as “publicly overlapping with Sandworm”) “very likely” was behind a series of attacks using the “Prestige” ransomware. “The Microsoft Threat Intelligence Center (MSTIC) has identified evidence of a novel ransomware campaign targeting organizations in the transportation and related logistics industries in Ukraine and Poland utilizing a previously unidentified ransomware

payload. We observed this new ransomware, which labels itself in its ransom note as “Prestige ransomware”, being deployed on October 11 in attacks occurring within an hour of each other across all victims.” Microsoft continues:

- “The enterprise-wide deployment of ransomware is not common in Ukraine, and this activity was not connected to any of the 94 currently active ransomware activity groups that Microsoft tracks
- “The Prestige ransomware had not been observed by Microsoft prior to this deployment
- “The activity shares victimology with recent Russian state-aligned activity, specifically on affected geographies and countries, and overlaps with previous victims of the FoxBlade malware (also known as HermeticWiper)”

[\(Microsoft attributes ‘Prestige’ ransomware attacks on Ukraine and Poland to Russian group - The Record by Recorded Future\)](#)

November 11, 2022 – CERT-UA posts information about a recent ransomware incident involving software called Somnia (Google translation): “The Government Computer Emergency Response Team of Ukraine CERT-UA has taken measures to investigate the information security incident, which resulted in a violation of the integrity and availability of information due to the use of malicious software Somnia. Responsibility for unauthorized interference in the operation of automated systems and electronic computers of the target of attack was assumed by the group FRwL (aka Z-Team), whose activity is monitored by CERT-UA by the identifier UAC-0118. [\(CERT-UA\)](#)

November 11, 2022 – Reuters reports: “The German government has earmarked an extra 1 billion euros (\$1.03 billion) from its 2023 budget to support Ukraine, with money allocated to defending against Russian cyberattacks and collecting evidence of war crimes.” The issue is part of an increasingly hot political debate over whether to increase aid to Ukraine, with the new allocation counted as a win for the Greens, the coalition party that has been the most active supporter of helping the embattled country. [\(Germany allocates extra 1 bln euros to Ukraine cyber-defence, documenting war crimes | Reuters\)](#)

November 13, 2022 – The *Wall Street Journal* reports that Russia’s troop mobilization has created a measurable “drag” on the country’s economy, particularly in the tech sector where about one quarter of the IT work force has reportedly left the country. [\(Departure of Tech Workers Weighs on Russian Economy - WSJ\)](#)

November 14, 2022 – *Lawfare* posts a podcast interview with Ukraine’s deputy minister of digital transformation, Georgii Dubynski, recorded on November 10 at a Hewlett grantee convening. Dubynski discusses the origins and mission of his agency, describes the range of Russia’s attacks since 2014, and assesses the effectiveness of both Russian and Ukrainian cyber operations. [\(The Lawfare Podcast: Georgii Dubynskyi on Ukraine’s Cybersecurity - Lawfare \(lawfareblog.com\)\)](#)



November 14, 2022 – Killnet posts an item on its Telegram channel saying they have attacked a section of the FBI’s website. The impact is unclear and the FBI has not yet provided comment. Another entity, RADIS, is reportedly tied to the event; its connection to Killnet is not known. ([Russian Hackers Claim Cyber Attack On FBI Website \(newsweek.com\)](#))

November 14, 2022 – CIA Director William Burns and Russian foreign intelligence chief Sergei Naryshkin meet in Turkey, reported to be the highest-level bilateral contact since Russia’s invasion of Ukraine. Naryshkin and U.S. Chargé d’Affaires in Moscow Elizabeth Rood tell RIA news agency no negotiations took place. Naryshkin adds: “I can note that the most frequently used words at this meeting were ‘strategic stability’, ‘nuclear security’, ‘Ukraine’ and ‘Kyiv regime’.” It is not clear whether the two spy chiefs discussed cyber issues. ([Putin's spy chief says he discussed Ukraine with CIA director | Reuters](#))

November 15, 2022 – An explosion in the Polish village of Przewodow kills two people. Initial reports, including from a senior U.S. intelligence official, point to Russia as the culprit but later information increasingly suggests it was probably an errant Ukrainian air defense missile, as Polish President Andrzej Duda himself remarks the following day. President Joe Biden tells journalists “it is unlikely” the missile came from Russia, based on analyses of its trajectory. (The Cipher Brief, 11-20-2022)

November 16, 2022 – Volodymyr Zelensky suggests that members of the G20 learn from Ukraine’s experiences in cyber defense. After briefly describing his country’s approach, he says: “If you or your allies and partners do not already have such a system and such digital protection, we will be happy to help you build them!” He adds that cyber defense is about “cooperation.” ([Zelensky speech — Official website of the President of Ukraine](#))

November 16, 2022 – Mieke Eoyang, deputy assistant secretary of defense for cyber policy, tells an Aspen Cyber Summit that Russia has “underperformed expectations” in Ukraine. “I think we were expecting much more significant impacts than what we saw.” Part of the explanation, she suggests, could be that Russia underestimated how long it takes to prepare for cyber operations ahead of a military engagement: “What you see in the data is the fact that Russia was not prepared for the conflict to go on as long as it did.” ([Russia’s cyber forces ‘underperformed expectations’ in Ukraine: senior US official | The Hill](#); [The Aspen Institute Cyber Summit \(aspencybersummit.org\)](#))

November 16, 2022 – Further comments by Mieke Eoyang, deputy assistant secretary of defense for cyber policy at the Aspen Cyber Summit delve into the Pentagon’s current takeaways from the war in Ukraine. Eoyang’s remarks are reported in detail by Mark Pomerlau in a DefenseScoop article the same day. “This is a really important conflict for us in the Department of Defense to understand,” Eoyang says, “because what you’re seeing is a cyber-capable adversary bring those capabilities to bear in the context of an armed conflict.” “One of the things that we’re seeing is the

context of the armed conflict dwarfs the cyber impacts of that.” “Things the Russians tried to disrupt via cyber ... did not have the strategic impact that they wanted. They sought to destroy those things physically.” “When you think about the cybersecurity of data centers, for example, it’s not just about patching and closing those things. It is about the physical security of those data centers. It is about whether or not those data centers are within the range of Russian missiles. Ukrainian colleagues that I had the privilege of meeting with, had a very different physical and visceral reaction to data centers that were above ground than that I think they would have had prior to the conflict. I think we have to think about it very differently.”

Pomerlau writes: “The war has also introduced the specter of non-state actors — on both sides — that can have a much larger impact in the operating environment. Unlike the insurgencies the U.S. saw during the wars in Afghanistan and Iraq where in some cases ordinary citizens took up arms, the Ukraine conflict is demonstrating that non-state actors also wield significant capability in the cyber realm.”

According to Eoyang, “In cyber, you do see non-state actors who have capability that can rival that of state actors. It does mean that it becomes a very complicated thing to defend against.” “One of the assumptions that I think those of us who work in traditional theories of armed conflicts have to understand is different about cyber [is] whereas in regular warfare, offensive capabilities are held monopoly to the state — you don’t have a lot of non-state actors who have theater missile defense systems or theater missile systems.” As DefenseScoop notes, that is not the case with cyber. ([How the war in Ukraine is forcing DOD to think differently about armed conflict and cyber's impact \(defensescoop.com\)](#); [The Aspen Institute Cyber Summit \(aspencybersummit.org\)](#))

On a related point, Eoyang spotlights the connection between kinetic conflict and cybersecurity. “When you think about cybersecurity as a risk-managed exercise, and one of the risks you are trying to manage in the context of that is armed conflict, you have to think very differently about what you are dealing with ... When you think about the cybersecurity of data centers, for example, it is not just about patching and closing those things. It is about the physical security of those data centers. It is about whether or not those data centers are within the range of Russian missiles.” ([Data centers are physical and digital targets, says Pentagon’s Eoyang \(c4isrnet.com\)](#))

November 16, 2022 – Mieke Eoyang, deputy assistant secretary of defense for cyber policy, also discusses the information environment in Ukraine during remarks at the Aspen Cyber Summit. A notable lesson from the conflict is that Ukrainians have managed to fend off a superior Russian capability in the information sphere. “We also now have to think about what it means for Ukrainians to be able to continue to communicate with the world. Because the ability of average Ukrainians to tell their story on TikTok, on Twitter, on Facebook, to share video of what has happened to them has denied Russia the information environment that they want to prosecute this conflict,” Eoyang says. “You can see Russia trying to take away from Ukraine the ability to control its own fate and its [digital] traffic by trying to reroute traffic through Russia as they take over territory.” According to DefenseScoop, Eoyang

adds that the fact that ordinary citizens can post their stories online marks a significant difference from other conflicts. ([How the war in Ukraine is forcing DOD to think differently about armed conflict and cyber's impact \(defensescoop.com\)](#); [The Aspen Institute Cyber Summit \(aspencybersummit.org\)](#))

November 16, 2022 – The *Wall Street Journal* reports on the findings of the Independent Anti-Corruption Commission, a Kyiv-based NGO, that an estimated three-quarters of the components of Iranian drones brought down in Ukraine were manufactured by Western companies. Ukrainian forces recently managed to hack a Mohajer-6 drone and land it intact, the paper reports. The U.S. government is said to have begun an investigation. ([Ukrainian Analysis Identifies Western Supply Chain Behind Iran's Drones - WSJ](#))

November 17, 2022 – CyberScoop reports that a revised version of the Trump-era National Security Policy Memorandum-13, which granted the U.S. military expanded authorities regarding the conduct of operations in cyberspace, is on its way to President Biden for review. After a several-month interagency process, according to sources, the updated draft document reportedly would allow the Defense Department to retain broad powers to launch cyber operations but would also require advance White House notification and the opportunity for agencies to register concerns with what is being planned. Supporters of DOD's enhanced ability to conduct operations say NSPM-13 has produced tangible results in Ukraine while critics have flagged the potential for adverse impacts on human rights, diplomacy, and private-sector infrastructure, CyberScoop notes. ([Biden set to approve expansive authorities for Pentagon to carry out cyber operations \(cyberscoop.com\)](#))

November 18, 2022 – Cyber Partisans, the Belarusian hacktivist group, announces on Twitter and Telegram that it has hacked the Russian General Radio Frequency Center (GRFC), a component of Russian telecommunications agency Roskomnadzor. "The work of the chief Kremlin censor has been disrupted," the group claims. "We also have a huge amount of material proving large-scale surveillance on the network and attempts to establish total control over everyone who has spoken out against the Putin regime over the past 20 years." The GRFC confirms the attack but denies that any employee workstations have been encrypted. (Risk Biz News, 11-20-2022)

November 18, 2022 – Killnet is believed to start targeting hospitals on or about this date, according to members of the Microsoft Azure Network Security Team. The number of attacks rises from 10-20 daily to 40-60 per day by February 17, 2023. (See also December 22, 2022, entry.) ([Pro-Russia hackers are increasingly targeting hospitals, researchers warn \(therecord.media\)](#))

November 18, 2022 – *Click Here*, a production of The Record Media, posts a podcast with representatives of the Cyber Defense Assistance Collaboration (CDAC), a group of representatives of several large Western cyber firms and nongovernmental organizations that has existed since 2009. The program discusses what it took – the

Russian invasion of Ukraine – to finally push forward the idea of public-private partnerships in cybersecurity. ([EXCLUSIVE: Rounding up a cyber posse for Ukraine - The Record by Recorded Future](#); [The Network — CDAC Network](#))

November 19, 2022 – Olga Stefanishyna, Ukraine’s deputy prime minister for European and Euro-Atlantic integration, voices concerns over Elon Musk’s reliability as a guarantor of Starlink services to Ukraine. Speaking to reporters at the Halifax International Security Forum, she says: “We have the Twitter guarantee of Elon Musk that he’s going to finance [Starlink], and he talked to our minister of digital transformation, so we consider it as a deal.” But she adds that Twitter is already becoming “the major source of manipulation” [as rendered by Breaking Defense] under Musk, who is “test[ing] the manipulation limits he can use ... Given this huge range of instability in the position of SpaceX CEO, from willingness and then to unwillingness to continue financial support [of Starlink], we’re doing, sort of, a contingency planning for ourselves.” ([Top Ukrainian official raises concerns about Elon Musk's 'manipulation' of information - Breaking Defense](#))

November 20, 2022 – Foreign Policy online publishes a piece titled “Billionaires Won’t Save Ukraine’s Internet.” It examines the experience Ukraine has had with Elon Musk and Starlink (see various entries above). Although Musk’s initial involvement was widely deemed extraordinarily important for Ukraine, the authors take a critical stance on his subsequent public actions and comments – while simultaneously drawing lessons for other conflicts. “Musk’s mercurial internet persona and the inconsistency of his support for Starlink terminals in Ukraine expose the disadvantages of relying on private actors for sustainable connectivity solutions in a rapidly changing geopolitical climate. Fighting wars has always involved gaining control over the enemy’s communication infrastructure, and we can expect adversarial connectivity to be an issue in future armed conflicts. Building a truly resilient internet requires states to invest in reliable infrastructure and modern cyberdefense that is proofed against attacks by adversaries—and contradictory takes from uninformed Twitter users.” ([Ukraine Can't Depend on Musk and SpaceX's Starlink for Internet \(foreignpolicy.com\)](#))

November 21, 2022 – Blackberry reports that the Russia-linked Gamaredon APT, which has ties to Russia and is also known as Shuckworm, IRON TILDEN, Primitive Bear, WinterFlounder, and ACTINIUM, has been exploiting Microsoft Office documents to attack Ukraine’s government and military. The method works even when Microsoft Word security features are enable, Blackberry reports. ([Gamaredon Leverages Microsoft Office Docs to Target Ukraine Government and Military \(blackberry.com\)](#))

November 21, 2022 – Slovak security firm ESET Research detects a new ransomware active in Ukraine that it calls #RansomBoggs. The company notifies Ukraine’s cyber authorities. ([\(10\) ESET Research on Twitter](#))

November 21, 2022 – Reuters posts an interview with retired U.S. General Ben Hodges, commander of U.S. Army forces in Europe from 2014-2017, who argues that



protecting major infrastructure from cyberattacks is as crucial as setting up missile defenses. He says the NotPetya attack of 2017 “was when I realized how vulnerable we are. If we can’t use [the port of] Bremerhaven, it will be very difficult for the United States to reinforce and to fulfil its part of operation plans.” ([Cyber as important as missile defences - ex-NATO general | Reuters](#))

November 22, 2022 – Killnet announces it has hit the official website of the Prince of Wales, among other targets, prompting media responses downplaying the magnitude and seriousness of the DDoS attacks. ([Killnet DDoS hackers target Royal Family and others \(computerweekly.com\)](#))

November 22, 2022 – Oleksandr Potii, deputy chairman of Ukraine’s SSSCIP, tells *Politico* about what he calls a new approach to cyberattacks – one that targets Ukrainian popular morale. “Classic cyberattacks, phishing, distributed denial-of-service (DDoS) threats, ransomware on critical infrastructure, these cyberattacks continue, but we have a new method of cyberattack: to influence political processes, social processes, civil society and political society. To destabilize the social-political situation in different countries, cities, and regions” around the world. “The most worrying impact is that due to these attacks, there is an influence on the public, public opinion and feelings. Destabilization of the sociopolitical situation in the country and in the regions is actually the aim of these attacks,” he says. “This is the direction of cyberattacks now and in the future.” ([Russia’s online attacks target Ukrainians’ feelings – POLITICO](#))

November 2022 – Meta releases a “Quarterly Adversarial Threat Report” for the third quarter of 2022. The report includes data on fake accounts tied to the U.S. military, as reported by Graphika and the Stanford Internet Observatory on August 24, 2022 (see July-August entry above). The activity includes “39 Facebook accounts, 16 Pages, two Groups and 26 accounts on Instagram.” “About 22,000 accounts followed one or more of these Pages, about 400 accounts joined at least one of these Groups and around 12,000 accounts followed one or more of these Instagram accounts.” “Although the people behind this operation attempted to conceal their identities and coordination, our investigation found links to individuals associated with the US military.” ([Quarterly-Adversarial-Threat-Report-Q2-2022-1.pdf \(fb.com\)](#))

November 22, 2022 – Sixteen U.S. Senators write a letter to Secretary of Defense Lloyd Austin expressing concern over reports the Biden administration has turned down repeated requests by Ukraine for MQ-1C Gray Eagle drones. (Text of letter, 11-22-2022)

November 22, 2022 – The Bell, an outlet with the Twitter description “The most important politics and business stories from Russia,” posts the results of an investigation into the background and personnel behind the anonymous Telegram channel “Rybar,” which reportedly has 1.1 million followers. “Of all the pro-Russian channels, Rybar is the most important source of information for analysts and the media.” The article

says that Rybar's data "is regularly used by CNN and Bloomberg." ([Unmasking Russia's influential pro-war 'Rybar' Telegram channel — The Bell — Eng](#))

November 23, 2022 – The European Parliament passes a resolution declaring Russia a state sponsor of terrorism, reported as a significant if purely symbolic vote. ([www.europarl.europa.eu; European Parliament declares Russia a 'state sponsor of terrorism' as Putin launches fresh attacks on Ukraine – POLITICO](#))

November 23, 2022 – Shortly after the European Parliament's vote on Russia, EP President Roberta Metsola tweets: "The @Europarl\_EN is under a sophisticated cyberattack. A pro-Kremlin group has claimed responsibility. Our IT experts are pushing back against it & protecting our systems. This, after we proclaimed Russia as a State-sponsor of terrorism." ([\(10\) Roberta Metsola on Twitter](#))

November 23, 2022 – Russian forces launch a new round of missile strikes against Ukraine and neighboring Moldova. NetBlocks tweets: "Confirmed: #Ukraine is in the midst of a nation-scale power blackout with high impact to internet access; live metrics show national connectivity now at 35% of previous levels after the second barrage of targeted missile Russian attacks in a week." The group adds that the missile attack "has impacted most regions." ([Internet disruptions registered as Russia moves in on Ukraine - NetBlocks](#))

November 23, 2022 – Reflecting another unanticipated side effect of the digital age, Bellingcat offers a guide on "How to Maintain Mental Hygiene as an Open Source Researcher." Noting the upside of the significant rise in public interest in exposing topics like war crimes in Ukraine, the outlet warns that researchers are likely to confront images that are "extremely graphic: they show the painful, disfiguring effects that war has on human bodies, cities and nature." More than that, Author Giancarlo Fiorella points out that "certain sounds, hateful text, or far-right imagery" can also have a very negative impact especially over time and he provides several tips for building mental and emotional "resilience." ([How to Maintain Mental Hygiene as an Open Source Researcher - bellingcat](#))

November 24, 2022 – The Czech National Cyber and Information Security Agency announces it is in the final stages of drafting legislation aimed at minimizing risks associated with third party suppliers of information and communications technology. The legislation follows numerous attacks on critical infrastructure in recent years. ([National Cyber and Information Security Agency - The Czech Republic enters the final phase of drafting legislation to reduce the risks associated with suppliers of information and communication technology. \(nukib.cz\)](#))

November 24-26, 2022 – Ukrainian government agencies organize a National Defense Hackathon, a three-day event attended by some 300 participants from a wide array of backgrounds. It takes place in the Kyiv Metro system which is safe from missile strikes and has reliable access to electricity, according to a media report. The hackathon's website lists the U.S. State Department and NATO among the

organizers. ([National Defence Hackaton \(Mil.Gov.Ua\); Ukraine's Volunteer Cyber Army Could Be Blueprint for the World: Experts \(newsweek.com\)](#))

Among the topics of discussion is the role of unofficial cyber operators like the IT Army and the need to improve the regulation of cyberspace. “Any army must have a legal status,” according to Ukrainian lawmaker Oleksandr Fediienko. “Otherwise, the world may consider it a terrorist organization.” Fediienko says that the Russian government is gathering evidence for lawsuits against Ukrainians. An article in *The Record* covering the hackathon discusses the larger issues involved. ([Should Ukraine rein in its patriotic hackers? - The Record by Recorded Future](#))

November 25, 2022 – *Fortune* reports that Yandex, “Russia’s Google,” wants to sell off its Russian businesses and “flee the country” in order to avoid Western sanctions. One observer points out the potential impact for Russia given Yandex’s advanced R&D work on AI and robotics, among other things. ([November 26, 2022 - by the grugq - The Info Op \(substack.com; Yandex to sell Russian businesses, flee country with its best tech | Fortune\)](#))

November 25, 2022 – The *Times* of London posts a piece on the rising prominence of drone warfare, noting that some 40 countries have drone forces, a function of the obvious benefits of relatively low costs and the protection of remote operation. ([Drones over Ukraine are reinventing war | Comment | The Times](#))

November 25, 2022 – Ukrainian officials announce that Iranian military advisers have been killed in Crimea.

November 25, 2022 – Australia’s Treasurer Jim Chalmers announces his government will begin to be more discriminating about who it allows to invest in the country’s important critical minerals sector. “Foreign investment is a good thing when it’s in our national interest,” he says, noting that Russia’s invasion of Ukraine has underscored the benefits of not having to rely on a dominant supplier. ([Australia to become 'more assertive' on foreign investment in critical minerals | Reuters](#))

Late November 2022 – Microsoft identifies a new ransomware variant, “Sullivan,” in use against Ukrainian targets. The company attributes it to Russia. ([Is Russia regrouping for renewed cyberwar? - Microsoft On the Issues](#))

November 28, 2022 – The Cyber National Mission Force releases a brief overview of its “hunt forward” operation in Ukraine in late 2021 and early 2022. “In addition to conducting a hunt forward on the ground, the team provided remote analytic and advisory support using new and innovative techniques, and conducted network defense activities aligned to critical networks.” ([Before the Invasion: Hunt Forward Operations in Ukraine > U.S. Cyber Command > News](#))

November 28, 2022 – The EU adopts a new directive on network and information systems. Called NIS2, it replaces an existing directive and aims to strengthen risk and incident management as well as cooperation across the union. ([EU decides to](#)

[strengthen cybersecurity and resilience across the Union: Council adopts new legislation - Consilium \(europa.eu\)](#)

November 28, 2022 – NSA cybersecurity director Rob Joyce gives a lengthy interview to *Politico's* Morning Cybersecurity. Touching on Ukraine, Joyce says Moscow has been “pretty specific” with respect to offensive hacking and have tried to “constrain[] their impacts inside Ukraine.” He sees the Viasat hack as something of an exception that proves the point because even though it had effects beyond Ukraine’s borders it was still “very much confined to the near-abroad of the Ukrainian conflict.” ([NSA cyber director talks threats, opportunities - POLITICO](#))

November 28, 2022 – NATO’s “flagship” annual cyber exercise begins in Tallinn. Cyber Coalition 2022 runs through December 2. Twenty-six member states participate including representatives from the private sector and academia. Col. Bernd Hansen, branch head for Cyberspace at NATO Allied Command Transformation, tells *Politico* that against the backdrop of the war in Ukraine, “There is a level of seriousness added; it’s not anymore so fictitious. It has become quite obvious those things [kinetic strikes and cyberattacks] are happening in reality.” ([Exercise Cyber Coalition 2022 Concludes in Estonia :: NATO's ACT; NATO prepares for cyber war - POLITICO](#))

November 29, 2022 – King’s College London posts an analysis, “Drones and defence innovation in Ukraine: consolidating wartime ingenuity,” by Julia Muravska, which highlights innovation as a lesson of the war. “This culture of innovation has proven effective, and sometimes decisive, on the battlefield. Importantly, it can support a robust domestic defence industrial base, essential for Ukraine’s long-term security.” ([Drones and defence innovation in Ukraine: consolidating wartime ingenuity | Feature from King's College London \(kcl.ac.uk\)](#))

November 29, 2022 – Reuters writes that a U.S.-Russian “deconfliction line” of communication on Ukraine, set up in March 2022, has been used once since Russia’s invasion. The report provides no details as to when or why it happened. The line is one of several modes of communication the two countries’ militaries have. This one, roughly equivalent to the hotline of Cold War days, runs between the U.S. European Command and Russia’s National Defense Management Center, the report says. Former U.S. Ambassador to Moscow Alexander Vershbow tells Reuters the line is intended to focus on daily operations rather than strategic discussions. He compares it to the communication link in use in connection with the conflict in Syria. ([Exclusive: U.S., Russia have used their military hotline once so far during Ukraine war | Reuters](#))

November 29, 2022 – A paper entitled “Sludge for Good” by four experts including two from NSA proposes inverting the concept of “sludge,” one usually bearing negative connotations, and using it to “maximize” perpetrators’ time and resources, thus raising the costs of an attack. The authors use the example of financial sanctions against Russia after its February invasion of Ukraine as a case of “successfully



imposed cost, both monetary and psychological,” which they say has hindered some attacks. ([2211.16626.pdf \(arxiv.org\)](#); [Investigating Lapsus\\$ \(fedscoop.com\)](#))

November 30, 2022 – The European Court of Human Rights renders several rulings on jurisdictional, evidentiary, and other matters in the “Case of Ukraine and the Netherlands v. Russia” dating back to 2014. The significance of the decisions is pointed out later by Bellingcat in an article that describes how the use of open source evidence was used and treated in the case. (Bellingcat compiled some of the materials that Ukraine ended up using in court.) ([UKRAINE AND THE NETHERLANDS v. RUSSIA \(coe.int\)](#); [How Open Source Evidence was Upheld in a Human Rights Court - bellingscat](#))

November 30, 2022 – AvengerCon VII, billed in a media report as “This year’s premier military hacker conference,” convenes today and December 1. Conference co-organizer Capt. Jacob Heybey tells DefenseScoop the informal theme will be crowdsourcing conflict, adding, “the Ukraine conflict was at the top of our minds when we picked this theme out — and the various efforts of the Ukrainian IT army and folks doing OSINT publicly on Twitter and the general phenomenon of people affecting global events as a general public.” ([AvengerCon military hacker conference to examine ‘crowdsourcing conflict’ \(defensescoop.com\)](#))

November 30, 2022 – The Vatican’s website suffers a DDoS attack. The Catholic News Agency notes that the perpetrators’ identity is unclear but that “the apparent attack” on the Vatican’s “aging” main site “comes a day after Russian leaders criticized Pope Francis for comments he made about Russia’s war in Ukraine in a recent interview.” ([Risky Biz News: CryWiper hits Russian courts and mayor offices in data-wiping attacks \(substack.com\)](#); [The Vatican says it’s been hacked — again | Catholic News Agency](#))

November 30, 2022 – Moldova and Ukraine experience interruptions in electricity service and the Internet after Russian strikes against Ukraine’s energy infrastructure. More than half of Moldova lost electricity and Ukraine’s Internet availability decreased by almost 65%. ([Ukraine and Moldova suffer internet disruptions after Russian missile strikes - The Record by Recorded Future](#))

November 30, 2022 – The *Wall Street Journal* prints an interview with a former hacker who operated from Russia in the 2000s and who now monitors Russian ransomware activity for Recorded Future Inc. Danny Smilyanets tells the outlet: “When Russia attacked Ukraine, some groups there declared loyalty to the Russian government. ...Those groups, they consist not only of Russian criminals. They consist of former Soviet Union bloc citizens, including [from] Ukraine.” He continues: “I don’t see Russia asking them directly because that’s not what’s really happening. What I see, a lot of groups who made some money with ransomware, they decided to be loyal to the state and create hacktivism. Instead of making money, they create destruction, they develop new ransomware payloads that have no intention to decrypt. That’s malware to disrupt the network, not to ask for ransom. That’s growing,

unfortunately. This war caused a lot of hatred on both sides, people just jumping into this boat of hacktivism without thinking of consequences.” ([Reformed Russian Cybercriminal Warns That Hatred Spreads Hacktivism \(wsj.com\)](#))

Late 2022 – An analysis apparently presented to U.S. military leaders in this timeframe reports that Russian operators of fake online accounts claim their attempts to manipulate social media and search engine rankings are picked up only about 1% of the time, according to leaked documents on the chat app Discord. The *Washington Post* reports that this information prompts “alarm” from experts it has consulted about the revelation, although one scholar, Thomas Rid of Johns Hopkins SAIS, believes the figure is probably either exaggerated or misleading. ([Russia claims bots are caught only 1% of the time, Discord leak says - The Washington Post](#))

December 2022 – The Ukrainian government begins jamming Russian satellite TV signals in occupied parts of the country, according to BBC Monitoring. Speeches by President Zelensky and other content are broadcast on Russian channels that have been fooled into relaying Ukrainian uplinks. ([Risky Biz News: Ukraine jams Russian satellite TV stations in occupied territories \(substack.com\)](#); [Chris Greenway on Twitter](#))

December 2022 – Officials and energy industry representatives from the United States and half a dozen European countries meet in Warsaw for a training session on cyber defenses, according to Deputy National Security Adviser Anne Neuberger. European participants came from the Czech Republic, Germany, Lithuania, Netherlands, Slovakia. The Idaho National Laboratory led the session, which focused on protecting industrial control systems, hardware and software. The idea came up during a conversation at a recent ransomware summit between Neuberger and a Polish official.

December 2022 – The executive committee of the Nordic Council meets. One result, reported the following month, is that the group of Nordic states will develop a common cybersecurity strategy focused on defense. Responsibility will fall to the Nordic Defense Cooperation (NORDEF), the primary body for joint military collaboration between the various Nordic armed forces. “Cybersecurity issues are more relevant than ever,” according to said Erkki Tuomioja, the Nordic Council’s president for 2022. “In recent years, the number of serious cyberattacks has grown. Additionally, the war in Ukraine has a direct effect on the Nordic region on many different levels. All these factors serve the need to have a common Nordic cybersecurity strategy.” ([Nordic states to develop common cybersecurity strategy \(defensenews.com\)](#))

December 1, 2022 – Google announces a series of new commitments to help Ukraine, including donating 50,000 1-year Google Workspace licenses to the government to help with protection of data systems, and a \$2 million grant and a Google.org Fellowship to the East Europe Foundation. The announcement coincides with a visit by Ukrainian vice prime minister and digital information minister Mykhailo Fedorov

to the company's offices in Washington, D.C. ([New ways we're supporting Ukraine \(blog.google\)](#))

December 1, 2022 – *Lawfare* posts an analysis of “Private-Sector Cyber Defense in Armed Conflict” by Stephanie Pell, which includes a focus on the role of Microsoft among other firms in Ukraine. ([Private-Sector Cyber Defense in Armed Conflict - Lawfare \(lawfareblog.com\)](#))

December 2, 2022 – The EU announces it has finally delivered equipment for a cyber lab, security software, and hardware to Ukraine's Armed Forces, under the European Peace Facility. The support program was announced on December 15, 2021 (see entry). ([Ukraine: EU sets up a cyber lab for the Ukrainian Armed Forces | EEAS Website \(europa.eu\)](#))

December 2, 2022 – The *Washington Post* publishes an interview with Mykhailo Fedorov, vice prime minister of Ukraine and minister of digital information, who supplements earlier comments and information about Ukraine's ongoing efforts to manage the reported thousands of cyberattacks it faces on a daily basis.

Among other points raised, the *Post* notes that while observers have praised Ukraine's effective information efforts, the country has come up against an unexpected obstacle in Facebook owner Meta, which Fedorov says has blocked the accounts of media that cover the war. He says his government has reached out to Meta, and that “[t]he situation is better now than it used to be, but it is still difficult.” ([Ukraine gets by in cyberspace with a little help from its friends - The Washington Post](#))

December 2, 2022 – *PwnAllTheThings* posts a lengthy report on successful Russian efforts to use Telegram to surveil Ukrainians. Building off a *Washington Post* story about a Ukrainian resistance fighter named Ihor who was detained and tortured by Russian forces in Kherson in August, the report details (and theorizes) how Ihor's captors tracked his Telegram communications with a Ukrainian special forces officer named “Smoke.” Along the way, the report sharply faults Telegram for allegedly knowingly maintaining inadequate security protections. ([Russia is spying on Telegram chats in occupied Ukrainian regions. Here's how. \(pwnallthethings.com\)](#); [Stealthy Kherson resistance fighters undermined Russian occupying forces - The Washington Post](#))

December 2, 2022 – *Lawfare* posts an analysis by Valentin Weber of the German Council on Foreign Relations on the benefits and risks associated with “extending weapons deliveries to the cyber domain.” He argues, among other points, that it is “not yet too late” for Ukraine “to conclude an agreement with NATO countries that lays out the provisions for sharing” and points to NATO's Sovereign Cyber Effects Provided Voluntarily by Allies (SCEPVA) as a precedent. He adds that “Shipping offensive cyber capabilities comes with its own set of challenges and risks,” such as making NATO members “co-belligerents,” which calls for methods to mitigate those potential problems. ([The Benefits and Risks of Extending Weapons Deliveries to the Cyber Domain - Lawfare \(lawfareblog.com\)](#))

December 3, 2022 – Ukraine’s Vice Prime Minister Mykhailo Fedorov tweets: “Thanks to Clearview AI and personally to Hoan Ton-That for the strong ongoing support of Ukraine. As of now, over 900 people from 7 UA government agencies used Clearview AI conducting over 125,000 searches. The newest global tech & our bravery — the win strategy for Ukraine.” The post includes a photo of Fedorov with company CEO Hoan Ton-That. ([\(10\) Mykhailo Fedorov on Twitter](#))

December 3, 2022 – Microsoft’s Digital Threat Analysis Center reports that “in the wake of Russian battlefield losses to Ukraine this fall, Moscow has intensified its multi-pronged hybrid technology approach to pressure the sources of Kyiv’s military and political support, domestic and foreign.” The report concludes the aim of the attacks is to undermine Western political support for Ukraine rattle the confidence of Ukrainian citizens. Microsoft anticipates several possibilities in the coming months. Among them are a continuing “cyber offensive” against Ukrainian critical infrastructure; more incidents outside Ukraine on the model of the recent Prestige ransomware-style attack in Poland; and “cyber-enabled influence operations” targeting Europe “in parallel with cyberthreat activity.” ([Preparing for a Russian cyber offensive against Ukraine this winter - Microsoft On the Issues](#))

Two weeks later, the Carnegie Endowment releases a report by Jon Bateman on Russia’s wartime cyber operations in Ukraine (see December 16, 2022, entry below), which takes issue with some aspects of Microsoft’s analysis. In early January, *Seriously Risky Business* further challenges Microsoft’s assessment that Russia is coordinating its cyber and conventional attacks, which in turn triggers a Twitter exchange. ([Microsoft’s Dull Bulb Fails to Illuminate - by Tom Uren \(substack.com\)](#); [\(23\) Dan Black on Twitter](#))

December 5, 2022 – Yevgeny Silkin, speaker of the Joint Forces Command for Strategic Communications of the Armed Forces of Ukraine, asserts that Iranian Shahed-136 kamikaze drones cannot perform properly in very cold conditions because they are made of plastic and similar materials, according to Ukrainian news outlet UNIAN. He says that no drone activity has been detected since November 17. ([Russia's Deadliest Drones Not Designed for Winter Cold, Ukraine Claims \(newsweek.com\)](#))

December 5, 2022 – Drones hit two military bases hundreds of miles inside Russia, reportedly in response to Russia’s missile strikes against Ukrainian infrastructure. Moscow acknowledges only one of the strikes, in Ryazan, but downplays its impact while video footage purportedly of the second attack shows evidence of a fireball at the Engels base near Saratov. Although Ukrainian officials do not claim responsibility, Zelensky adviser Mykhailo Podolyak posts a suggestive tweet the same day: “The Earth is round – discovery made by Galileo. Astronomy was not studied in Kremlin, giving preference to court astrologers. If it was, they would know: if something is launched into other countries’ airspace, sooner or later unknown flying objects will return to departure point.” ([Ukraine Drones Target](#))



[Military Bases Deep in Russia, Showing Expanded Reach - The New York Times \(nytimes.com\)](#); (9) Михайло Подоляк on Twitter)

A later report indicates the Pentagon has tacitly endorsed Ukraine's long-range strikes after revising its threat assessments of the war in the wake of Russia's now-daily attacks against civilians. ([Pentagon gives Ukraine green light for drone strikes inside Russia | News | The Times](#))

December 5, 2022 – The IT Army's Telegram channel adds 1,080 new subscribers, as noted by cyber expert Stefan Soesanto, who adds that "the channel has been losing ~100 subscribers daily since its peak in March 27." ((9) [Stefan Soesanto on Twitter](#))

December 5, 2022 – Russia has covertly been using U.K. and U.S. organizations to target Ukraine, according to a new report by cybersecurity firm Lupovis. "The findings from our study were shocking. The most concerning revealed that Russian criminals have hijacked the networks [of] UK, US, French, Brazilian and South African businesses, including a Fortune 500 outfit, and over 15 healthcare organisations to launch attacks on Ukraine." Lupovis, based in Scotland, advertises that it uses nonconventional "cyber deception products" to help companies fend off attacks. In this case, the firm built five decoys including a "honey files service" designed to lure Russian threat actors. Some 50-60 attackers targeted the decoys, often "within a minute of them going live." Attacks included reconnaissance; attempts to recruit them into bots; SQL injection; remote file inclusion; Docker exploitation; usage of leaked Ukrainian credentials; and use of known CVEs, the report says. ([Russia compromises major UK and US organisations to attack Ukraine | Lupovis](#))

December 5, 2022 – Secretary of Homeland Security Alejandro Mayorkas warns in a speech that "our homeland security has converged with our national security." As evidence, he points to the NotPetya incident in 2017 and the Russian attack against U.S. satellite company Viasat in February 2022, noting that cyberattacks can be initiated "with a keystroke." The speech is before the Center for Strategic and International Studies. ([DHS secretary says US faces 'a new kind of warfare' \(cyberscoop.com\)](#))

December 5, 2022 – Recorded Future's Insikt Group publishes a lengthy report "exposing TAG-53's credential harvesting infrastructure used for Russia-aligned espionage operations." TAG-53's infrastructure "likely overlaps with other infrastructure tactics, techniques, and procedures (TTPs) previously attributed to Callisto Group, COLDRIVER, and SEABORGIUM, who have been linked to activity aligning with Russian state interests." Among its key judgments, Insikt finds: "TAG-53 has used domains masquerading as organizations across multiple industry verticals, with a particular focus on government, intelligence, and military industries." ([Message from Recorded Future](#))

December 6, 2022 – VTB, Russia's second largest, state-owned bank, reports: "The bank's technological infrastructure is under an unprecedented cyber attack from abroad ... The largest not only this year, but in the whole time the bank has operated." The IT

Army of Ukraine claims credit for the incident. ([Russian state-owned bank VTB hit by largest DDoS attack in its history | Reuters](#); [IT Army of Ukraine on Twitter](#))

December 7, 2022 – U.N. Secretary-General Antonio Guterres announces the U.N. is looking into charges that Iran has provided drones to Russia and will send relevant findings to the Security Council. A 2015 UNSC resolution governing the Iran nuclear deal (the Joint Comprehensive Plan of Action) imposed an arms embargo on Iran until October 2020, but Western governments have argued that certain military technologies are still covered until October 2023. Guterres himself recently reported that Iranian transfers of drones or ballistic missiles with a 300-kilometer range would require advance approval by the Council. ([West presses U.N. chief to inspect drones used by Russia in Ukraine | Reuters](#))

December 7, 2022 – *The Cyber Defense Review* publishes an analysis by Herbert Lin of the use of offensive cyber operations in the war in Ukraine. The study focuses at length on questions about cyber's utility as a coercive tool and a warfighting instrument. ([Lin-Russian Cyber Operations in Ukraine-Cyber Defense Review-2022-fall.pdf](#))

December 7, 2022 – Kim Zetter posts an article on the risks private security firms face in providing assistance to one or another side in a conflict. Noting that Microsoft, Mandiant, Cisco, ESET, Recorded Future, and other companies have openly provided support to Ukraine that would be standard practice in ordinary times, “experts say the same activities conducted in the midst of war introduces legal complications and raises the risk that security workers, infrastructure and customer data could become targets of Russia, who might view them as legitimate military targets.” The article discusses issues such as how to define a direct participant in a war and numerous relevant concepts such as “defense vs. offense,” “distinction,” and “qualified neutrality.” ([Security Firms Aiding Ukraine During War Could Be Considered Participants in Conflict \(substack.com\)](#))

Matt Tait of *PwnAllTheThings* (and formerly of GCHQ) posts an item the following day praising Zetter and her article but disagreeing that executives and personnel at Western firms run a significant risk of being considered participants in the Ukraine war. He includes a discussion of various provisions of international law. ([No, Tech Companies and Cybersecurity Firms Aren't Close to Becoming Direct Participants in the Conflict by Helping Ukraine \(pwnallthethings.com\)](#))

December 7, 2022 – The Kiel Institute, an independent (Federal Government-funded) foundation in Schleswig-Holstein, updates its informative Ukraine Support Tracker, “a database of military, financial and humanitarian aid to Ukraine.” Information covers the period January 24 through November 20, 2022. The site notes that Europe has recently surpassed the United States in aid commitments to Ukraine with Germany leading the continent. The EU total is almost 52 billion euros compared to the U.S. at just below 48 billion euros. ([Ukraine Support Tracker | Kiel Institute \(ifw-kiel.de\)](#))

December 8, 2022 – CERT-UA receives information from cybersecurity specialists to the effect that e-mails have been disseminated with the slug “How to recognize a kamikaze drone” and purporting to be sent on behalf of the State Emergency Service of Ukraine. ([CERT-UA](#))

December 8, 2022 – Estonia’s disproportionately large role in providing assistance to Ukraine on cyber and technology matters is detailed in *Politico*. ([How Estonia is helping Ukraine take on Russian cyber threats - POLITICO](#))

December 8, 2022 – American basketball player Brittney Griner is released from Russian prison in exchange for arms dealer Viktor Bout. CNN reports a few days later that U.S. officials floated the names of two cyber criminals, Alexander Vinnik and Roman Seleznev, as possible trades for ex-Marine Paul Whelan, but Moscow declined. ([Griner freed: WNBA star swapped for Russian, heads home | AP News](#); [Paul Whelan: Russia demanded a spy held in Germany be freed in exchange for the American | CNN Politics](#); [The Cybersecurity 202: Cybercriminals were in the mix for the Russia prisoner swap - mbyrne@email.gwu.edu - The George Washington University Mail \(google.com\)](#))

December 9, 2022 – The Defense Department announces its latest military aid package for Ukraine. Totalling \$275 million, it will include technology to counteract Russian drones. ([New \\$275M Ukraine assistance package includes more counter-drone weapons \(defensescoop.com\)](#))

December 9, 2022 – Cloud Atlas, described as a cyber-espionage group first discovered in 2014, is profiled by Check Point Research. The latter reports that not much has changed with the group except for a significant narrowing of its scope of activities to Russia, Belarus, and conflict areas in Ukraine and Moldova. ([Cloud Atlas targets entities in Russia and Belarus amid the ongoing war in Ukraine - Check Point Research](#))

The Check Point Research article also links to another technical analysis of Cloud Atlas (by Positive Technologies) that provides additional details: [APT Cloud Atlas: Unbroken Threat \(ptsecurity.com\)](#)

Noting these two assessments, the grugq newsletter adds the following commentary that touches on the debate over the most effective uses of cyber in a conflict. “The more important lesson to learn here is that espionage is more useful than effects operations conducted without context. What I mean by that is, effects operations are most effective when employed within a strategy that takes advantage of them. Effects operations executed at random are generally speaking of negative value — they train the opposition and burn access. Intelligence is almost always useful. Effects are useful inside a strategic context. Information operations are orthogonal because they typically don’t involve the same resources. This focus on espionage demonstrates that Ukraine is focussed on getting the most value from their limited resources. They don’t have the same sort of cyber forces available as the Russians. Ukraine has limited resources and must get maximum value from

what they have. That means espionage.” ([December 10, 2022 - by the grugq - The Info Op \(substack.com\)](#))

December 9, 2022 – The *Wall Street Journal* reports that power grid operators in Europe are alarmed at the shortage of cybersecurity experts needed to protect the sector in a period of greatly heightened threat since Ukraine switched from Russia’s electric grid to Europe’s after the Russian invasion in February . “The worry is about cascading effects,” a Polish official says. “We are in the worst situation ever.” ([European Electricity Sector Lacks Cyber Experts as Ukraine War Raises Hacking Risks \(wsj.com\)](#))

December 11, 2022 – According to data provided by GPSJam, numerous urban areas in Russia experience a jump in GPS disruption starting today. Experts tell *Wired* it may be a Russian attempt to block additional long-range Ukrainian drone attacks after the strikes earlier this week. “In addition, wireless data analytics firm Aurora Insight measured an increase in GPS signal levels in the area at the start of December—a sign that potential GPS interference could have happened.” ([GPS Signals Are Being Disrupted in Russian Cities | WIRED](#))

December 11, 2022 – Based on Ukraine’s experience, an item in *The Australian* concludes that Australia is already in the midst of a cyberwar and warns of the possibility of “incredible damage” to basic infrastructure. ([Telstra apologises for accidentally publishing data of thousands of customers online | Foxconn to invest US\\$500 million in India | Why is Twitter shutting down Chinese activists' accounts? \(substack.com\); https://www.theaustralian.com.au/business/australia-is-already-in-the-midst-of-a-cyberwar/news-story/9a43964303bc1e90c4be62e3ad6780a6](#))

December 12, 2022 – The port of Odesa is hit by Russian drone attacks that leave 1.5 million people and non-critical infrastructure without power. President Zelensky says it might take several days to restore electricity fully under sub-zero weather conditions, although the port itself resumes operations within a day. The BBC reports that Russia used 15 Iranian-made drones around Odesa and Mykolaiv. Ukrainian military sources say they shot down 10 of them. ([Ukraine war: Odesa port reopens after energy network hit - BBC News](#))

December 12, 2022 – Ukraine’s Ministry of Digital Transformation signs a memorandum of understanding with Australian firm Internet 2.0, based in Canberra, providing for training of Ukrainian war veterans in cybersecurity. ([ASPI Dec 12 \(substack.com\); Russia-Ukraine war: Australian company Internet 2.0 training Ukrainian veterans in cybersecurity \(afr.com\)](#))

December 12, 2022 – A new Carnegie Endowment study, “Cyber Operations in Ukraine: Russia’s Unmet Expectations,” tackles the question of Russia’s underwhelming offensive cyber performance in Ukraine. Author Gavin Wilde starts by analyzing Russia’s doctrinal concepts of “information confrontation” or “information war/warfare” – which differ from the West’s conception of “cyber” – then offers



three hypotheses to help explain Russia's unimpressive showing to date. One is that Moscow's information operations forces have only been in existence for 6-8 years and focuses mainly on counterpropaganda. The second is that Russia's "special services" have generally not evolved sufficiently from traditional roles to be competitive in 21<sup>st</sup> century operations and are further encumbered by inter-service rivalries (e.g., between the GRU and FRB). The third is that Moscow underperformed in the crucial initial phases of the conflict for a combination of reasons, including a lack of resources, exaggerated assumptions about the level of support they would receive in eastern Ukraine, excessive secrecy surrounding invasion planning, and a general overestimation of their own relative capabilities. ([202212-Wilde RussiaHypotheses-v2.pdf \(carnegieendowment.org\)](#))

December 13, 2022 – Graphika and the Stanford Internet Observatory Cyber Policy Center publish a new report, "Bad Reputation," about Russian troll farms. "Suspected Russian actors have leveraged alternative social media platforms to target right-wing U.S. audiences with divisive political narratives to a greater extent than previously known," the authors write. The report describes 35 recently found "inauthentic accounts" on Gab, Gettr, Parler, and Truth Social that are mirroring foreign influence operations (IO) dating back to at least 2020. (One short-lived account masqueraded as belonging to a Kid Rock fan.) "The newly-identified activity illustrates the extent to which suspected Russian actors are able to leverage social media platforms that lack robust policies on foreign IO." ([Bad Reputation \(graphika.com\)](#))

December 13, 2022 – Reuters publishes a special report on the continuing flow of technology imports into Russia despite U.S. and EU restrictions. "A joint investigation by Reuters and the Royal United Services Institute (RUSI), a London-based defense think tank, details for the first time the global supply chain that continues to feed Russia with Western computer components and other electronics. The investigation into this trade identified a galaxy of obscure importers and exporters, like [Turkish firm] Azu International, and found that shipments of semiconductors and other technology continue to arrive in Russia from Hong Kong, Turkey and other trading hubs." ([The supply chain that keeps tech flowing to Russia \(reuters.com\)](#))

December 13, 2022 – Former NSA Director Keith Alexander tells an audience he believes Vladimir Putin "will use [cyber] clearly before nuclear." Speaking at the Cyber Initiatives Group Winter Summit, the ex-USCYBERCOM head adds: "If he uses nuclear, he's dead .... I believe that will cause NATO to rethink [whether] they're in or out." Alexander says Russia has not stopped considering cyberattacks. "I think there will be more." ([Putin to choose cyber warfare before nuclear weapons, former NSA chief says | The Hill](#))

December 13, 2022 – An official Ukrainian government website posts an article describing the growth of "military-oriented IT" in the country because of the war and providing details about several specific examples. "Today, a regular serviceman of the Armed

Forces of Ukraine (AFU) can name about a dozen most widespread software and applications that are used by the military on the daily basis: Kropyvva, MilChat, Delta, GisArta, Terminal, ComBat Vision, Virazh Planshet, and more.” Cyber expert Stefan Soesanto tweets: “Combine that with Starlink, Palantir's MetaConstellation, ClearView and other Western products, and the scale of the digital battlefield is immense.” ([Digital weapons of war: applications and software that help Ukraine to win; \(19\) Stefan Soesanto on Twitter](#))

December 14, 2022 – Russia launches its first major drone attack on Kyiv in several weeks. Officials report shooting down 13 of the Iranian Shahed devices, known locally as “mopeds.” ([Ukraine shoots down drones as Russia says no 'Christmas ceasefire' on the cards | Reuters](#))

December 15, 2022 – One day after Poland’s Sejm votes 231-2 with one abstention to designate Russia a state sponsor of terrorism, the parliament’s website is hit by a DDoS attack, which Warsaw attributes to the pro-Russian group NoName057(16). ([Ukraine War and Upcoming SEC Rules Push Boards to Sharpen Cyber Oversight \(wsj.com\)](#); [Poland warns of attacks by Russia-linked Ghostwriter hacking group \(bleepingcomputer.com\)](#))

December 15, 2022 – NSA releases its Cybersecurity Year in Review 2022. Cyber Director Rob Joyce introduces the document to reporters, warning against complacency about Ukraine, particularly in the energy sector. “As the war progresses there’s certainly the opportunities for increasing pressure on Russia at the tactical level, which is going to cause them to reevaluate, try different strategies to extricate themselves.” ([NSA cyber director warns of Russian digital assaults on global energy sector \(cyberscoop.com\)](#))

December 15, 2022 – The *New York Times* uses leaked emails from the All-Russia State Television and Radio Company (VGTRK), made public by DDoSecrets, to put together an article on how Russian state media cherry picks from (right-wing) American and Chinese media to create disinformation about the state of the war in Ukraine. ([An Alternate Reality: How Russia’s State TV Spins the Ukraine War - The New York Times \(nytimes.com\)](#))

December 15, 2022 – Reuters publishes a lengthy article based on an investigation the wire service has been conducting with iStories, a Russian media outlet, in collaboration with the think tank Royal United Services Institute in London. The probe “has uncovered a logistical trail that spans the globe” and leads to the Special Technology Centre in St. Petersburg, Russia, described as the production line for the Orlan 10 “Sea Eagle” drone, which the Ukrainian military says are used daily to attack Ukrainian positions killing up to 100 troops per day. ([Exclusive: The global supply trail that leads to Russia’s killer drones | Reuters](#))

December 15, 2022 – Mandiant reports on a malware operation targeting the Ukrainian government. “Threat activity tracked as UNC4166 likely trojanized and distributed

malicious Windows Operation system installers which drop malware that conducts reconnaissance and deploys additional capability on some victims to conduct data theft.” Mandiant is not yet able to attribute the malware to a particular group.

“However, UNC4166’s targets overlap with organizations targeted by GRU related clusters with wipers at the outset of the war.” ([Trojanized Windows 10 Operating System Installers Targeted Ukrainian Government | Mandiant](#))

December 16, 2022 – Japan releases “National Security Strategy of Japan,” which notes that Russia’s aggression against Ukraine has easily breached the very foundation of the rules that shape the international order. The possibility cannot be precluded that a similar serious situation may arise in the future in the Indo-Pacific region, especially in East Asia.” The document includes a section on cybersecurity which pledges the government to strengthen its capabilities to levels “equal or surpassing ... leading Western countries.” In addition to routine security measures, “Japan will introduce active cyber defense” that foresees giving the government “the necessary authorities to allow it to penetrate and neutralize attacker’s servers in advance to the extent possible.” This will entail restructuring the National Center for Incident Readiness and Strategy for Cybersecurity (NISC) in order to centralize cybersecurity policies. ([security strategy en.pdf \(mod.go.jp\)](#); [\(20\) TweetDeck \(twitter.com\)](#))

December 16, 2022 – The Carnegie Endowment releases “Russia’s Wartime Cyber Operations in Ukraine: Military Impacts, Influences, and Implications” by Jon Bateman. The 78-page report aims to “help bridge the divide between cyber-specific and general military” analyses of the war, most of which, the author points out, omit any mention of the other field. ([Russia’s Wartime Cyber Operations in Ukraine: Military Impacts, Influences, and Implications - Carnegie Endowment for International Peace](#))

December 16, 2022 – *Foreign Policy* publishes an article assessing “Whatever Happened to Russia’s Vaunted Cyberoffensive?” ([Whatever Happened to Russia’s Vaunted Cyberoffensive? \(foreignpolicy.com\)](#))

December 17, 2022 – The Center for Innovations and Development of Defense Technologies of the Ministry of Defense of Ukraine informs CERT-UA about phishing e-mails coming from a compromised e-mail address of an employee of the Ministry of Defense. The phishing messages aim at infecting users of the “Delta” situational awareness system (see October 27, 2022, entry above) with malware. ([CERT-UA; Ukraine’s DELTA military system users targeted by info-stealing malware \(bleepingcomputer.com\)](#))

December 19, 2022 – In the early morning, Russia launches another drone attack on Kyiv. Ukrainian officials say the Air Force shot down between 20 and 30 out of 35 drones, although the attack succeeded in hitting power plants, electrical systems, and other sites. ([Russia-Ukraine War: Putin Discusses ‘Unified’ Defense With Belarus During Visit to Its Capital - The New York Times \(nytimes.com\)](#); [Russian drones strike Kyiv’s power grid in third attack in a week | Reuters](#))

December 19, 2022 – U.S. deputy representative to the United Nations Robert Wood expresses disappointment the U.N. Secretariat has so far not initiated an investigation into Western charges that Iran has been supplying Russia with weaponized drones for use against Ukraine, allegations Tehran and Moscow vehemently deny. Wood says U.N. leaders are “apparently yielding to Russian threats.” ([US and Iran clash over Russia using Iran drones in Ukraine | AP News](#))

December 19, 2022 – *Washington Post* columnist David Ignatius in Kyiv describes observing Ukrainian forces utilizing Western high-tech tools to identify and track Russian battlefield targets. Discussing the “wizard war” (or “algorithmic warfare”) in detail, he concludes that Ukrainian bravery coupled with access to “the most advanced intelligence and battle-management software ever seen in combat” means “the Russians probably can’t win this war.”

However, he adds that although many CEOs and others consider this “the good war,” the “aggressive” use of cyber tools “obscures many important questions: How dependent should countries be on entrepreneurs whose policy views could change? We can applaud the use of these tools in ‘good’ wars, but what about bad ones? And what about private tools being turned against the governments that helped create them?”

Following up his own questions, he writes: “But after spending weeks investigating the new tools developed by Palantir and other companies, the immediate takeaway for me is about deterrence — and not just in Ukraine. Given this revolution in technology, adversaries face a much tougher challenge in attacking, say, Taiwan than they might imagine. The message for China in this emerging digital battle space is: Think twice.” ([Opinion | How the algorithm tipped the balance in Ukraine - The Washington Post](#))

December 19, 2022 – Carnegie Endowment experts post an overview of what Russia’s invasion of Ukraine should lead us to expect in terms of future cyber conflict. ([What the Russian Invasion Reveals About the Future of Cyber Warfare - Carnegie Endowment for International Peace](#))

December 20, 2022 – White House NSC spokesman John Kirby tells reporters the Biden administration is assessing Ukraine’s air defense needs, hinting that additional drone support may be included. ([White House hints at sending more counter-drone systems to Ukraine \(defensescoop.com\)](#))

December 20, 2022 – Palo Alto Network’s Unit 42 releases a report on activities of the FSB-tied APT group Trident Ursa (aka Gamaredon, UAC-0010, Primitive Bear, Shuckworm). The unit has “mapped out over 500 new domains, 200 samples and other Indicators of Compromise (IoCs) used within the past 10 months that support Trident Ursa’s different phishing and malware purposes.” ([Russia’s Trident Ursa \(aka Gamaredon APT\) Cyber Conflict Operations Unwavering Since Invasion of Ukraine \(paloaltonetworks.com\)](#))



December 20, 2022 – Ukraine’s Deputy PM Mykhailo Fedorov tells Bloomberg his government has struck a deal with SpaceX to provide 10,000 additional Starlink antennas over the next few months. ([Ukraine Reaches Deal with Elon Musk’s SpaceX to Receive More Starlink Antennas - Bloomberg](#))

December 20, 2022 – Ukraine’s Cyber Police announce the dismantlement of another 13 bot farms with over 1.5 million accounts said to be aimed at promoting pro-Russian narratives, among other activities. ([Cyberpolice conducted a nationwide operation to stop the activities of enemy bot farms — Department of Cyberpolice](#))

December 20, 2022 – The Guardian suffers a “serious IT incident” late in the night that disrupts various pieces of the company’s infrastructure and services, the company reports. In early January, staff members are told offices will remain closed for at least a month. The situation is described as a “total nightmare” with financial, payroll, printing, and other services affected. While the reason for the incident is unconfirmed, one outlet speculates: “It can also be fairly said that reporting on major international incidents such as Russia’s war on Ukraine may leave a title exposed to malicious actions by Russia-backed or aligned groups.” [Guardian hit by serious IT incident believed to be ransomware attack | The Guardian | The Guardian](#); [Fallout from Guardian cyber attack to last at least a month | Computer Weekly](#); The CyberWire, 1-6-2023)

December 21, 2022 – President Biden announces the United States will send Ukraine a Patriot missile battery. The largely symbolic gesture is one element of a package of almost \$2 billion in additional security aid to Ukraine. ([White House Says President Zelensky Set Security Parameters for His Visit to the U.S. \(substack.com\)](#))

December 21, 2022 – President Zelensky delivers a historic address to Congress. (Video at [Watch Volodymyr Zelensky’s full speech to US Congress | CNN](#))

December 21, 2022 – On the same day that Zelensky addresses Congress, Vladimir Putin announces a significant boost to Russian military forces, including troops, equipment, and hardware. Upgrading communications capabilities is listed among other measures. ([Putin to Boost Russian Military, Signaling Protracted War in Ukraine - WSJ](#))

December 21, 2022 – Ukraine’s IT Army is compiling a “Book of Executioners” consisting of data on Russian soldiers in Ukraine, Deputy PM Mykhailo Fedorov tells Bloomberg in a story today. ([Ukrainian Hackers Gather Data on Russian Soldiers, Minister Says - Bloomberg](#))

December 21, 2022 – The *Wall Street Journal* publishes an interview with Victor Zhora, deputy chief of Ukraine’s SSSCIP. He begins: “We are facing tens of cyber incidents daily. That means that they have a lot of resources, that they are seeking opportunities every day. Their strategy is seeking vulnerabilities, is providing attempts to gain persistence in networks, attempts to exfiltrate data, attempts to

disrupt services in Ukrainian government entities, the telecom sector, critical information infrastructure and seeking impact that they can bring to all the infrastructure. That's the strategy, an opportunistic strategy, a chaotic strategy, but a strategy that is focused on harming Ukraine, on bringing impact to our economy, to our infrastructures, to our everyday life, and to our resilience." ([Ukraine's Cyber Units Aim to Retain Staff, Keep Services Stable as War Enters Year Two \(wsj.com\)](#))

December 22, 2022 – (Date approx.) The CyberPeace Institute releases its Quarterly Analysis Report for Q3 (July-September 2022), "Cyber Dimensions of the Armed Conflict in Ukraine." The report begins: "The CyberPeace Institute documented 178 cyber incidents against entities in Ukraine between January and September 2022. With 87 incidents impacting 17 sectors in Q3, there has been a 248% increase in incidents compared to the previous quarter. This increase is driven by a significant increase in DDoS attacks targeting organizations in Ukraine." ([Cyber Dimensions Ukraine Q3 Report.pdf \(cyberpeaceinstitute.org\)](#))

December 22, 2022 – The Department of Health and Human Services Health Sector Cybersecurity Coordination Center (HC3) posts an Analyst Note indicating that the pro-Russian group KillNet has recently started targeting the healthcare industry. ([202212221500 KillNet Analyst Note TLPCLEAR \(hhs.gov\)](#))

December 23, 2022 – A day after Senate approval, the House of Representatives passes a \$45 billion aid package for Ukraine, part of a \$1.66 trillion government funding bill that will go to President Biden for his signature. The U.S. has already sent about \$50 billion of aid to Ukraine in 2022. ([US Approves Patriot Missiles, New \\$45B Aid Package for Ukraine \(voanews.com\)](#))

December 22, 2022 – Ukrainian cybersecurity expert Alex Holden and a team at Hold Security have broken into Solaris, a large Russian online drug market, and siphoned off \$25,000 worth of bitcoin, according to Forbes today. Holden, a Wisconsin resident, says he is publicizing the hack in order to try to get Solaris to close its site. He has donated the bitcoin to Enjoying Life, a Ukrainian nonprofit that helps displaced persons from the war. The article says the attack may have wider implications including possibly disrupting the activities of Killnet, which has ties to Solaris. ([A Ukrainian Steals \\$25,000 In Bitcoin From Russian Dark Web Drug Market And Gives It To A Kyiv Charity \(archive.ph\)](#))

December 25, 2022 – The Speaker of Russia's Duma, Vyacheslav Volodin, writes on Telegram that the lower house is drafting legislation to raise taxes for Russians who leave the country. Some 700,000 people have reportedly fled since the September mobilization drive. Russians working outside the country are required to pay taxes independently.

A later report indicates that some lawmakers also want to ban remote work for some professions, including IT. But officials in the Digital Ministry reportedly worry that a complete ban could hurt Russian competitiveness in that sector. ([Duma](#)

[prepares higher taxation for Russians who left country - speaker | Reuters](#); [Russia-risks-causing-new-year-it-worker-flight | Reuters](#))

December 28, 2022 – Microsoft restores access to installations of Windows to individual users in Russia, according to sources cited by *Izvestia*. The outlet says that neither Microsoft nor its distributor, AllSoft, responded to requests for comment. ([Boot Day: Windows has again become available for download in Russia | Articles | News \(iz.ru\)](#); [Risky Biz News: Secure Boot not working on recent MSI motherboards \(substack.com\)](#))

December 29-30, 2022 – Russia launched attacks on Ukrainian cities overnight using more than a dozen drones. Ukraine says its forces shot down all 16 of the craft, said to be made in Iran. ([Russia Follows Ukraine Missile Barrage With Wave of Armed Drones - WSJ](#))

December 30, 2022 – A pro-Ukrainian Telegram channel posts a warning to the Islamic Republic of Iran, presumably in connection with its provision of drones to Russia that have just been used to strike Ukrainian targets: “And just to show off what we can, and what we cannot Ayatollah Khamenei personal website went down. Just for one hour. As we adviced, it is a warning. If we act, we will act much more rough, no regrets and no sorries there will be. Night timr, no harm. Just a demo. Next time we will deface it. Iranians, it is not your war, step down and fuck off. Coz next time there will be oil processing scada.” ([Telegram: Contact @cybersecs; Iran’s support of Russia draws attention of pro-Ukraine hackers - The Record from Recorded Future News](#))

December 30, 2022 – Poland’s Special Services department issues a statement highlighting increasing numbers of “computer incidents” against Polish targets and those of other states supporting Ukraine, undertaken by Russian hackers. One of the perpetrators in recent months is the threat group GhostWriter, which the Poles accuse of trying to spread Russian disinformation. ([Russian cyberattacks - Special Services - Gov.pl website \(www.gov.pl\)](#))

December 31, 2023 – From February 24 to this date, 3,292 transactions involving semiconductors took place involving Russia, according to Russian customs data examined by Nikkei Asia. Semiconductors in about 70% of the transactions were identified as U.S.-made. The total value for the period was \$740 million or more. Three-quarters of the shipments were from Hong Kong or mainland China. ([Special report: How U.S.-made chips are flowing into Russia - Nikkei Asia](#))

2022 – The year witnesses a 24% drop in stolen credit card volumes on Russia’s dark web, Mandiant’s Insikt Group reports. Analysts attribute the drop to Moscow’s early cybercrime crackdown followed by the invasion of Ukraine. ([Annual Payment Fraud Intelligence Report: 2022 \(recordedfuture.com\)](#))

2023

2023

2023

2023

2023

January 2023 – The SSSCIP of Ukraine publishes a report in Ukrainian titled “Vulnerability Detection System and Response to Cyber Incidents and Cyber Attacks.” According to an item on the SSSCIP website describing the findings of the report: “During 2022, with the help of the Vulnerability Detection and Response System for cyber incidents and cyberattacks, about 58 billion events were processed, obtained using the means of monitoring, analyzing and transmitting telemetry information about cyber incidents and cyberattacks, 181 million suspicious information security events were detected (in the initial analysis), 179 thousand critical information security events were processed (potential cyber incidents identified by filtering suspicious events of information security and secondary analysis), recorded and processed directly by security analysts of 415 cyber incidents.” ([sseb6a10-b7aa-4396-8b04-e0e4b7fca111.pdf \(scpc.gov.ua\)](#))

January 2023 – Around this time (possibly late 2022), dozens if not hundreds of leaked documents begin to appear on the messaging platform Discord. The documents, which include near-verbatim transcripts of highly classified materials on the war in Ukraine and other sensitive topics, initially circulate among a small group of about a dozen members before one of the group’s members posts some of them on other, more heavily trafficked sites. ([New Details on Intelligence Leak Show It Circulated for Weeks Before Raising Alarm - WSJ](#); [Discord member details how documents leaked from closed chat group - The Washington Post](#))

Early 2023 – (Date approx.) Russia begins jamming Starlink devices in Ukraine. The terminals are reported to be vulnerable to GPS jamming (they were not designed for the battlefield) although Ukrainian troops reportedly have come up with several ways to get around detection, which in turn leads to Russian adaptations in approach. For one, it is reported later that Moscow may be moving advanced jamming systems into the country, even though they are normally kept for defending Russian territory and are themselves vulnerable because of the need to be near their target and their lack of mobility. ([Using Starlink Paints a Target on Ukrainian Troops - Defense One](#))

January-March 2023 – According to European cybersecurity firm Thales, “in the first quarter of 2023, the overwhelming majority of [Ukraine-war-related] incidents (80.9%) have been inside the European Union” rather than in Ukraine itself. This is up from roughly a 50-50 split in Summer 2022. ([From Ukraine to the whole of Europe:cyber conflict reaches a turning point | Thales Group](#))

January-March 2023 – In the first quarter of 2023, Google’s Threat Analysis Group (TAG) continues to “disrupt campaigns from multiple sets of Russian government-backed attackers focused on the war in Ukraine.” Google’s blog notes that “Russian government-backed phishing campaigns targeted users in Ukraine the most, with the country accounting for over 60% of observed Russian targeting. Looking at



information operations (IO), our takedowns reflect a steady pattern of Russian attempts to circumvent our policies.” The report’s author notes examples of ways that different threat actors have been adapting to new conditions and obstacles. ([Ukraine remains Russia’s biggest cyber focus in 2023 \(blog.google\)](#))

January-March 2023 – Russian disruptive cyberattacks against Ukraine drop in frequency surge during this period, according to Mandiant. A senior manager at the firm theorizes that several factors are involved, including government crackdowns, the impact on cyber crime in Eastern Europe from the war in Ukraine, and improvements in preventive measures. ([Faltering against Ukraine, Russian hackers resort to ransomware: Researchers - Breaking Defense](#))

January 1, 2023 – Ukrainian missiles hit a Russian troop garrison in Makiivka (Donetsk) resulting in dozens of casualties (89 according to official Russian sources, but others say the total is far higher). Amid highly unusual state and social media coverage of memorial services, the Russian Defense Ministry blames rampant use of mobile phones by Russian troops for identifying the garrison’s location. Critics, including in Russia, say military commanders made numerous basic errors. ([Russian military leaders blamed for heavy losses in New Year's Day strike - The Washington Post](#))

The *New York Times* reports that despite previous experience and orders from higher up, both Ukrainian and Russian troops continue to use cell phones to call loved ones. ([Russian Troops’ Use of Cellphones Is a Persistent, Lethal Danger - The New York Times \(nytimes.com\)](#))

January 2, 2023 – A Ukrainian drone damages a power supply facility in the Klimovsky district of Russia’s Bryansk region, the governor reports later in the day. The facility is back up and running within 12 hours, he says. Reuters says it is not able to verify the report independently. ([Ukrainian attack cut power in Russian region for a time - governor | Reuters](#))

January 2, 2023 – President Zelensky announces that over the past two days Ukraine has shot down some 89 Iranian-made drones used by Russia to attack the country. He charges that Moscow is planning a “prolonged attack with Shaheds” probably aimed at exhausting Ukrainian air defenses and its population. A Defense Ministry report puts the total number of drones shot down at 1,880. ([Ukraine Shoots Down Nearly 90 Iranian-Made Drones in Two Days: Zelensky \(newsweek.com\)](#))

January 3, 2023 – The European Commission’s top cybersecurity official, Lorena Boix Alonso, gives an interview to the *Washington Post*’s Cybersecurity 202. Alonso, formally the director for digital society, trust and cybersecurity in the directorate general for communications networks content and technology, describes various dimensions of Europe’s response to the war in Ukraine, which has “pushed us to adapt our cybersecurity policy” and made the EC “more ambitious,” including passing and proposing new, wide-ranging legislation. ([Europe’s cybersecurity dance card is full - The Washington Post](#))

January 3, 2023 – Ukraine’s Cyber Police Department and Main Investigative Department of the National Police jointly took down a major phishing call center alleged to have defrauded some 18,000 people in Kazakhstan. They arrest 40 individuals including three alleged ringleaders in Dnipro. ([Ukrainian Cops Bust Prolific Fraud Call Center - Infosecurity Magazine \(infosecurity-magazine.com\)](#))

January 3, 2023 – ANC Pharmacy, one of Ukraine’s biggest pharmacy chains, announces it has partnered with Binance Ukraine to allow customers to use cryptocurrency to make payments online. According to Binance, such payments do not conflict with Ukrainian law, although a media article notes that “local laws do not allow direct payments in cryptocurrencies like Bitcoin.” ([Ukrainian pharmacies enable crypto payments via Binance Pay \(cointelegraph.com\)](#))

January 3, 2023 – The Associated Press reports that advances in drone warfare in Ukraine “have accelerated a long-anticipated technology trend that could soon bring the world’s first fully autonomous fighting robots to the battlefield, inaugurating a new age of warfare.” Citing military analysts, combatants, and AI researchers, the article notes: “That would mark a revolution in military technology as profound as the introduction of the machine gun.” ([Drone advances in Ukraine could bring dawn of killer robots | AP News](#))

January 3, 2023 – The *Wall Street Journal* describes Ukraine’s success in accomplishing within months what it took the United States and other powers years to achieve – and at far greater cost – building a digital warfighting capability. An array of off-the-shelf equipment starting with cheap drones and the ability to link those weapons and coordinate their missions through satellites and software are catalogued. Key lessons for future combatants, according to sources, include the ability to innovate, improvise, and tap the skills and resources of nonmilitary experts. ([Ukraine Has Digitized Its Fighting Forces on a Shoestring - WSJ](#))

January 3, 2023 – ABC News posts a story about a project known as “I Want to Live,” in Ukraine, which operates a hotline offering Russians (and Ukrainians who have fought on the Russian side) a way to surrender. More than 1 million Russians have reached out, say project personnel, either by phone, text, or by visiting the website; more than 4,000 people have actually asked to surrender. The process of surrendering involves gathering personal information for a potential defector and passing it to state or military authorities who evaluate it. A defector then travels to a pre-arranged spot where a drone makes visual contact and guides them to a safe passage route. ([Ukraine offers Russian soldiers a hotline to surrender - ABC News \(go.com\)](#))

January 3, 2023 – The *Wall Street Journal* reports that corporate boards are likely to develop closer working ties to, and oversight of, cybersecurity operations, a result of the war in Ukraine and the Covid-19 pandemic. Cybersecurity officers have increasingly seen their roles elevated as directors seek more specific information about the risks of attack, especially from foreign governments. “There’s a mindshift

change going on that nobody would be safe from a nation-state attack,” according to one Norwegian bank officer. ([Ukraine War and Upcoming SEC Rules Push Boards to Sharpen Cyber Oversight \(wsj.com\)](#))

January 5, 2023 – At 7:00 p.m. in the occupied territory of Kherson, Russian TV channels begin showing President Zelensky’s New Year’s address – the result of a hack by pro-Ukrainian elements. The address runs approximately eight times, according to someone in the territory. BBC Monitoring reports that the Ukrainian government has been jamming Russian signals in occupied areas since December. ([Risky Biz News: Ukraine jams Russian satellite TV stations in occupied territories \(substack.com\)](#); (20+) [Facebook](#); [Chris Greenway on Twitter](#))

January 5, 2023 – President Biden confirms to German Chancellor Olaf Scholz that the United States will provide Bradley armored vehicles to Ukraine as part of a \$2.85 billion aid package. Germany has pledged to supply its own Marder infantry fighting vehicles. Both have been high on President Zelensky’s wish list. ([US to send Bradley vehicles to Ukraine as part of new aid package | CNN Politics](#))

January 5, 2023 – President Putin calls for a 36-hour ceasefire to coincide with Orthodox Christmas. Kyiv rejects the idea while President Biden says he believes Putin is “trying find some oxygen” for his forces. Ukrainian officials later report that shelling around Bakhmut continued despite the Russian declaration. ([Putin's call for Orthodox Christmas truce in Ukraine greeted with scepticism | Reuters](#); [Shelling booms around Bakhmut in 'Christmas ceasefire' | Reuters](#))

January 5, 2023 – CISA Director Jen Easterly tells the Consumer Electronics Show in Las Vegas the threat of a significant Russian cyber hit against the United States is probably “not going to end anytime soon. We need to continue to be vigilant, keep our shields up, and ensure that we are putting all those controls in place.” She says that Russia miscalculated at the start of the war. “I think they thought it was going to be a quick and easy drive down to Kyiv.” But Moscow also “calculated well” that attacking U.S. infrastructure would be “very escalatory,” which may explain the absence of any such strikes to date. ([CISA director: US needs to be vigilant, 'keep our shields up' against Russia | The Hill](#))

January 5, 2023 – Moldova’s Information Technology and Cyber Security Service (STISC) sends out a notice about scam and phishing attacks against government institutions, saying over 1,330 messages have been sent to date. ([STISC: WARNING - \(gov.md\)](#))

January 5, 2023 – A news item reports Taiwan’s space agency is holding preliminary talks with a number of investors in hopes of funding a project to build an indigenous satellite communications system. Taiwan’s thinking is heavily influenced by Ukraine’s successes using Elon Musk’s Starlink network, according to the *Financial Times*. ([Taiwan plans domestic satellite champion to resist any China attack | Financial Times \(ft.com\)](#))

January 9, 2023 – Ukrainian officials are gathering evidence of what they call war crimes by Russia, which they are sharing with the International Criminal Court in the Hague, according to Victor Zhora, chief digital transformation officer, in an interview published today by Politico. “When we observe the situation in cyberspace we notice some coordination between kinetic strikes and cyberattacks, and since the majority of kinetic attacks are organized against civilians — being a direct act of war crime — supportive actions in cyber can be considered as war crimes,” Zhora says. ([Kyiv argues Russian cyberattacks could be war crimes – POLITICO](#))

In a separate interview, a fellow at the Geneva Academy of International Humanitarian Law and Human Rights, Lukasz Olejnik, disagrees with Zhora’s contention. “The issue is that those cyberattacks would have to be significant enough. Just targeting some infrastructure with low-key activities might not be sufficient,” he tells *Cyber Insights*. ([\(20\) Lukasz Olejnik \(@LukaszOlejnik@Mastodon.Social\) on Twitter](#))

The *Washington Post*’s Cybersecurity 202 later adds further discussion and quotes from legal experts. ([The war in Ukraine tests how cyberattacks fit into rules for war crimes - The Washington Post](#))

January 9, 2023 – National Security Adviser Jake Sullivan says that Iran’s provision of drones to Russian forces may be contributing to war crimes. “Their weapons are being used to kill civilians in Ukraine and to try to plunge cities into cold and darkness which, from our point of view, puts Iran in a place where it could potentially be contributing to widespread war crimes,” he tells reporters in Mexico. ([Iran could be contributing to war crimes by sending drones to Russia - White House | Reuters](#))

January 10, 2023 – An article in *The Record* reports on pro-Ukrainian leaks of Russian data, noting a “gigantic surge” of such leaks since Russia’s invasion and quoting a Ukrainian cyber expert as saying “Ukrainian hackers have data on almost every resident of Russia, even those who do not use a computer.” The aim of the almost daily leaks is said to be mainly to stir up anger in the Kremlin, attract new members to their groups, and distract adversaries. ([Pro-Ukraine hackers leak Russian data in hopes someone will make sense of it - The Record from Recorded Future News](#))

January 10, 2023 – The impact of crowdfunded technology on Ukraine’s war effort is explored in a fascinating article in the *Wall Street Journal*. Hundreds of small-scale operations run outside military procurement channels help supply troops with everything from encrypted radios to drones, often picked up on eBay by individuals in Western countries, shipped to Poland or other neighboring countries, then driven into Ukraine and from there to the front lines. A look at the website of one freelance supplier “provides insights into the activities of some of the 20 or so groups he equips. Donors—who come mostly from abroad—can give money to specific units. Money and equipment has come from a bar in Berlin and a woman in Florida who says she sold a rocking chair and blender to raise funds. One popular twist is allowing donors to write their messages on shells or vehicles and equipment they



paid to have fixed.” ([Crowdfunded Technology Gives Ukraine an Edge on Front Lines - WSI](#))

January 11, 2023 – An article in *Politico* asserts that Russian cyberattacks are intended to “break the will of everyday citizens and turn the tide of the war” after “widespread failures” on the battlefield. Later citing American and Ukrainian government sources as well as Western companies, the article catalogs events from the previous year, reporting that the “pace of cyberattacks directed against Ukraine has been unrelenting over the past 12 months” and that civilian facilities are increasingly being targeted. ([Russia's cyberattacks aim to 'terrorize' Ukrainians - POLITICO](#))

January 12, 2023 – Former NSA Deputy Director Rick Ledgett posts a brief comment on cyber issues he is paying attention to in the new year: “One thing that I’m watching is the activities of the Russian government around the Ukraine invasion, and in particular cyber activities.” He pronounces DDoS attacks against Poland attributed to the GRU as “significant” because they appeared to be aimed at impeding the country’s logistics and transportation, “presumably to interfere with their activities in support of the movement of supplies and weapons to Ukraine. It is a shift in targeting that may presage more intrusive and widespread cyber actions by Russia.” He adds there are some “unknowns” about the incident including whether it might presage attacks on “secondary or even tertiary targets” in other NATO countries. ([Q&A with Rick Ledgett \(cyberinitiativesgroup.com\)](#))

January 12, 2023 – General Aymeric Bonnemaïson, head of France’s Cyber Defense Command, tells a weekly press briefing that European allies of the United States who allow U.S. cyber teams to monitor their networks are leaving themselves open to spying by Washington. Bonnemaïson was apparently referring to the USCYBERCOM’s “hunt forward” teams that have been deployed to at least 18 countries as of last August. *Le Monde* reports that Bonnemaïson characterized U.S. operations as “relatively aggressive.” He reportedly made similar remarks at a closed meeting of the National Assembly’s Defense Committee in December. (*Le Monde* 1-13-2023, as reported in [Paris highlights risk from US cyber defense teams – Le Monde \(azerbaycan24.com\)](#); [Risky Biz News: Secure Boot not working on recent MSI motherboards \(substack.com\)](#))

January 12, 2023 – Chainalysis publishes its annual Crypto Crime Report which tracks illicit cryptocurrency activities around the world. The report notes that 2022 was “one of the most tumultuous in cryptocurrency history,” although outside of activity tied to sanctions (OFAC was hugely active last year), transaction volumes actually decreased during the year. Risky Biz News comments that one reason for this is the war in Ukraine. ([2023 Crypto Crime Trends: Illicit Cryptocurrency Volumes Reach All-Time Highs Amid Surge in Sanctions Designations and Hacking - Chainalysis](#); [Risky Biz News: Crypto-crime volumes went down in 2022, ransomware payments too \(substack.com\)](#))

January 12, 2023 – The U.S. Privacy and Civil Liberties Oversight Board holds a public forum on FISA Section 702. Gen. Paul Nakasone delivers the keynote in which, without mentioning names of countries, he asserts: “This authority provides the U.S. government irreplaceable insights, whether we're reporting on cybersecurity threats, counterterrorism threats, or protecting U.S. and allied forces.” The forum prefigures what is expected to be a congressional battle over whether to retain Section 702 in its current form. ([Section 702 Forum press release.pdf \(pclob.gov\)](#); <https://documents.pclob.gov/prod/Documents/EventsAndPress/44b0eb0f-5d52-4a0c-bf13-093a6c0f340f/Section%20702%20Forum%20press%20release.pdf>)

January 13, 2023 – The pro-Ukrainian hacker group DumpForums claims to have broken into and obtained data from Reg.ru, said to be the “largest Russian domain name registrar.” The group writes on their Telegram channel: “We failed to negotiate with Reg.ru. Today, no one will have any doubts that there really was a hack. We will start merging all developments, configs, etc. of the largest Russian domain name registrar and hosting provider. In fact, we have hacked them more than once, no matter what they do – we still managed to get back into their network. And now, when everything that was needed from their hosting is on our servers, we can kindly provide our audience with the downloaded information.” ([Telegram: Contact @dumpforums](#); [Risky Biz News: Secure Boot not working on recent MSI motherboards \(substack.com\)](#) )

January 13, 2023 – Kraken claims to have taken control of the Solaris marketplace, the second attack on the dark website in less than a month (see December 22, 2022, entry). But since Kraken, like Solaris, is reported to be pro-Kremlin, the motive is unclear but presumed not to be political. ([Risky Biz News: Dark web mega-hack as Kraken takes over Solaris \(substack.com\)](#))

January 13, 2023 – Scottish National Party MP Stewart McDonald, recipient of the order of merit from the Ukrainian government for his work on Ukraine, has his personal email account hacked. The U.K.’s NCSC believes the perpetrator is a group known as Seaborgium, which is thought to have ties to Russian intelligence and has previously hacked files and emails of former MI6 head Sir Richard Dearlove and journalist Paul Mason, according to the BBC. ([SNP MP Stewart McDonald's emails hacked by Russian group - BBC News](#))

January 14, 2023 – An update aggregating reports on “Russia’s hybrid war against Ukraine” appears in the CyberWire. It notes among other things that aside from Ukraine the most “uneasy” place in the Near Abroad is Moldova. (The CyberWire, 1-14-2023)

January 14-15, 2023 – (Date approx.) CIA Director William Burns travels secretly to Kyiv to brief President Zelensky on U.S. assessments of Russia’s military plans as well as the prospects for continued U.S. support for Ukraine during the current session of Congress. ([CIA director held covert meeting with Zelensky on Russia’s next steps - The Washington Post](#))

January 15, 2023 – Yuriy Shchychol, head of Ukraine’s State Service of Special Communications and Information Protection (SSSCIP), calls for a “Cyber United Nations” to provide “a hub or a venue where we can exchange information, support each other and interact.” *Politico* publishes Shchychol’s comments, part of an interview with the outlet, noting that the Ukrainian’s description of a global entity covering the “civilized world” almost certainly implies “the exclusion of Russia and its allies.” ([Ukraine calls for ‘Cyber United Nations’ amid Russian attacks - POLITICO](#))

January 15, 2023 – A report in SecurityLab.ru indicates that Intelligence has “secretly” restored access to its drivers to users in Russia, although registration is required and processes with a Russian IP address reportedly do not work. Intelligence stopped providing access in February 2022. ([Intel secretly returned to Russia \(securitylab.ru\)](#); [Risky Biz News: Secure Boot not working on recent MSI motherboards \(substack.com\)](#))

Mid-January 2023 – Russia-linked Nodaria group has been using malware called Graphiron (or Infostealer) from October 2022 till at least this time period, according to a Symantec report in early February 2023. The Nodaria espionage group (a.k.a. UAC-0056 and TA471) is said to be targeting Ukraine with the malware, which is “designed to harvest a wide range of information from the infected computer, including system information, credentials, screenshots, and files.” ([Graphiron: New Russian Information Stealing Malware Deployed Against Ukraine | Symantec Enterprise Blogs \(security.com\)](#); [Russian ‘WhisperGate’ hackers are using new data-stealing malware to target Ukraine | TechCrunch](#))

January 16, 2023 – Forces in Russian-controlled Sevastopol in the Crimea shoot down 10 drones in what authorities there call a “failed Ukrainian attack,” according to Governor Mikhail Razvozhayev. ([Russian-installed official in Crimea says air defences shot down 10 drones | Reuters](#))

January 16, 2023 – Kyiv Mayor Vitali Klitschko says the city’s infrastructure could collapse imminently under Russian missile attacks. ([Davos 2023: Russian bombing puts Kyiv's utilities under critical strain -Klitschko | Reuters](#))

January 16, 2023 – German Foreign Minister Annalena Baerbock calls for a special international tribunal to prosecute Russian leaders for war crimes in connection with Moscow’s invasion of Ukraine. ([Germany calls for special tribunal against Russia over Ukraine war | Reuters](#))

January 16, 2023 – Sometime this week, Latvia’s Ministry of Defense comes under a phishing attack, which the Latvians ascribe to Russia-based Gamaredon, noting the use of the latter’s domain name to send the malicious emails. ([Latvia confirms phishing attack on Ministry of Defense, linking it to Russian hacking group - The Record from Recorded Future News](#))

January 17, 2023 – Russian hackers reportedly delay a broadcast by Yuriy Shchyhol, head of Ukraine’s SSSCIP, in which he attempts to brief the press about Ukraine’s efforts to defend against cyber attacks. The SSSCIP initially “assumes that the cyberattack was waged by the UAC-0082 (Sandworm) group.” Later in the month, CERT-UA reports finding five malware samples: CaddyWiper, ZeroWipe, SDelete, AwfulShred, and BidSwipe. ([Washington's spy program fight \(axios.com\)](#); [The attack on Ukrinform might have been carried out by the Sandworm hacking group, associated with russian GRU: preliminary results of CERT-UA investigation \(cip.gov.ua\)](#); [CERT-UA](#))

January 17, 2023 – The Economic Security Council of Ukraine publishes a report jointly with other Ukrainian government and military departments and a private consulting firm, the TRUMAN Agency, assessing Russia’s hybrid war in Ukraine. The 48-page report, “Cyber, Artillery, Propaganda: Comprehensive Analysis of Russian Warfare Dimensions,” features a timeline of events and several recommendations. ([cip.gov.ua](#))

Cyber expert Lukasz Olejmik provides a detailed appraisal of the report, calling it “among the most important cybersecurity-related assessments released this year” (albeit it’s still only January). ([TechLetters Insights - Ukraine report highlighting the links between kinetic warfare and cyberattacks - is a new definition of aggression needed \(substack.com\)](#))

January 17, 2023 – Mandiant’s Insikt Group releases its “Annual Payment Fraud Intelligence Report” for 2022 noting a 24% drop in “card-not-present” stolen credit card data and a 62% fall in “card-present” data on Russia’s dark web for the year. ([Annual Payment Fraud Intelligence Report: 2022 \(recordedfuture.com\)](#))

January 18, 2023 – Australia’s Minister for Defence Personnel Matt Keogh says the government is “very conscious” of the possibility of cyber attacks as a result of its support of Ukraine but says Australia will not back down in the face of an “existential threat” to that country. ([Australia prepared for possible Russian cyber-attacks after troops sent to train Ukraine soldiers – as it happened | Australia news | The Guardian](#))

January 18, 2023 – Palantir CEO Alex Karp tells a World Economic Forum audience that his company is committed to supporting Western values against threats to democracy from the likes of Russia and China. Estimating that two-thirds of software developers in Silicon Valley are probably uncomfortable with working directly with the Defense Department, law enforcement or the intelligence community, Karp says his message to them is: “Don’t work here.”

Karp also discusses specific support Palantir has provided “philanthropically” to Ukraine. The company’s software, MetaConstellation, for example, has given Ukraine “targeting with like a factor of 20 better” than previously, he claims. MetaConstellation “allows you to use algorithms on large data sets to hone in on adversaries over, say, a whole country ... [with] the infusion of data from satellites, telephones, other sources, classified sources, and then the disambiguation of that so people only see what they are allowed to see on the



battlefield.” He adds that the software “took us 15 years to build in various forms.” ([Palantir CEO to those who don't support U.S. military work: 'Don't work here' \(defensescoop.com\)](#))

January 19, 2023 – Ukraine signs a technical agreement relating to its planned accession to the Cooperative Cyber Defence Centre of Excellence (CCDCOE), a NATO component based in Estonia. While the agreement requires approval of all members, it is expected. Membership will allow Ukraine access to advanced technology, research, and information to help defend itself from cyberattacks. ([Ukraine signs agreement to join NATO's Joint Cyber Defence Centre of Excellence \(cip.gov.ua\)](#); [Ukraine signs agreement to join NATO cyber defense center - The Record from Recorded Future News](#))

January 2023 – Starting roughly in mid-January, Lithuania comes under a series of phishing and email operations apparently attempting to sow doubt about the status of Ukrainian refugees in that country by implying that Lithuania was helping Ukraine to track refugees and send military-aged males back to fight in the war. Vilnius attributes the attacks to a “Russian cyber actor.” ([U.S., Europeans work to cripple Russia's spy networks across continent - The Washington Post](#))

January 21, 2023 – The Hill posts an item citing numerous experts on their expectations concerning Russian cyber operations for 2023. The Kremlin is likely to be more active in the face of military setbacks but there will probably be only “minor impact” given the likelihood that Ukraine and its allies will respond firmly, the report says. ([Russia expected to increase cyberattacks in Ukraine war — to little effect | The Hill](#))

January 23, 2023 – Ukraine and Finland sign a memorandum of understanding to promote exchanges on digitalization, information technology and cybersecurity. Expanding Ukraine’s digital resilience is the overall goal. ([Ukraine and Finland to cooperate in digitalization and digital resilience - Memorandum signed | Cabinet of Ministers of Ukraine \(kmu.gov.ua\)](#))

January 23, 2023 – The future of the IT Army of Ukraine is the subject of an item in *Wired*. “With a quarter of a million subscribers to the IT Army of Ukraine Telegram channel, and a bilingual website providing attack instructions, target statuses, command tools, and distributed denial of service (DDoS) bots, it’s not hard to see why [Western] governments have warned their citizens against joining. The problem is not that the cause is unjust but that there is no legal protection for civilians engaged in offensive cyber operations.” ([Hacktivism Is a Risky Career Path | WIRED](#); [Amateur hackers warned against joining Ukraine’s ‘IT army’ | Ukraine | The Guardian](#))

January 24, 2023 – The Microsoft Threat Intelligence Center’s Ukraine operations, which include monitoring 24 trillion signals daily and deploying a team of “hunters” to identify Russian attacks on Ukrainian networks, are discussed in an opinion piece in the *Sydney Morning Herald*. The article highlights the development of public-private partnerships that has taken place over Ukraine, although it includes criticisms of the

company. The writer comments that while Microsoft has been “indispensable to Ukraine in its hour of need,” the conflict has also allowed the company to “showcase” itself and “buff its political credentials.” Further, Microsoft’s “commitment to democracy only runs so far,” the writer alleges, pointing to its continued commercial involvement with China. ([The Russia-Ukraine war is forcing Big Tech to choose sides \(smh.com.au\)](#))

January 24, 2023 – A much more positive account (see previous entry) of Microsoft’s substantial role in helping Ukraine in its cyber conflict with Russia appears in *Computerworld* (although the article does note that “[b]y helping Ukraine, Microsoft also helps its customers — and it happens to be good PR, as well.” ([How Microsoft is helping Ukraine’s cyberwar against Russia | Computerworld](#))

January 24, 2023 – Cybersecurity firm Fortinet posts an update to its April 28, 2022 (see entry) backgrounder on wiper malware. Titled “The Year of the Wiper,” it takes their research through the end of 2022 and describes “how wiper malware and their attack scenarios have changed.” ([The Year of the Wiper | FortiGuard Labs \(fortinet.com\)](#))

January 25, 2023 – Defense Department Directive 3000.09, “Autonomy in Weapons Systems,” is released. Its chief purpose is described as follows: “Establishes policy and assigns responsibilities for developing and using autonomous and semi-autonomous functions in weapon systems, including armed platforms that are remotely operated or operated by onboard personnel.” An academic analysis of the document and a related NATO implementation plan (see October 13, 2022, entry) comments: “Both announcements reflect a crucial lesson militaries around the world have learned from recent combat operations in Ukraine and Nagorno-Karabakh: Weaponized artificial intelligence is the future of warfare.” ([DoD Directive 3000.09, "Autonomy in Weapon Systems," January 25, 2023 \(defense.gov\)](#); [War in Ukraine accelerates global drive toward killer robots \(theconversation.com\)](#))

January 25, 2023 – Killnet says it has targeted numerous German government websites, financial institutions, and airports with DDoS attacks in response to Berlin’s announcement that it will send Leopard tanks to Ukraine. ([Russian 'hacktivists' briefly knock German websites offline | Reuters](#))

January 25, 2023 – An article in *Lawfare* analyzes “Big Data and the Law of War,” but notes that while “big data is growing in significance” and may soon become an “object[] of international conflict, ... [s]o far it has not been front and center in Russia’s invasion of Ukraine.” ([Big Data and the Law of War - Lawfare \(lawfareblog.com\)](#))

January 25, 2023 – In a Tweet, the Breached cybercrime forum discloses that Yandex source code has been leaked. The code contains the source for Search, Maps, Taxi, Mail, Market, Travel, Cloud, Pay, and many other services, and all leaked files have the date February 24, 2022. (Risky Biz News, 1-26-2023)

January 25, 2023 – ESET uncovers a fresh malware attack on unnamed Ukrainian targets this week, which it ties to a well-known GRU hacking unit. “Attackers deployed a new wiper we named #SwiftSlicer using Active Directory Group Policy,” the group Tweeted. “We attribute this attack to #Sandworm.” ([Russia's Sandworm hackers blamed in fresh Ukraine malware attack | CyberScoop](#))

January 25, 2023 – In late 2022, the Defense Department promulgated an update to Directive 3000.09, “Autonomy in Weapon Systems,” with an effective date of today. A Lawfare analysis notes that for the previous decade, the directive has been “the primary U.S.-specific policy regarding the use of autonomous technologies in weapons systems.” The analysis points out that the prominence of AI on the battlefield in Ukraine makes the update “rather timely.” ([Decoding the Defense Department's Updated Directive on Autonomous Weapons - Lawfare \(lawfareblog.com\)](#))

January 26, 2023 – Dmitry Rogozin, former head of Roscosmos, declares that two entities, the Foundation for Advanced Research (FPI) and the company Android Technology, are building a combat version of the latter's Marker ground reconnaissance robot designed to destroy Abrams and Leopard tanks. A western expert calls the announcement a PR stunt. ([Robot "Marker" will be prepared for the destruction of NATO tanks - RIA Novosti, 26.01.2023; Russian Robot Maker Working On Bot to Target Abrams, Leopard Tanks - Defense One](#))

January 26, 2023 – The U.K.'s National Cyber Security Centre issues an advisory: “The Russia-based SEABORGIUM (Callisto Group/TA446/COLDRIVER/TAG-53) and Iran-based TA453 (APT42/Charming Kitten/Yellow Garuda/ITG18) actors continue to successfully use spear-phishing attacks against targeted organisations and individuals in the UK, and other areas of interest, for information gathering activity.” ([NCSC Advisory-SEABORGIUM-and-TA453](#))

January 26, 2023 – The FBI reports that it has disrupted the Hive ransomware group after six months of work. The Bureau then tweets: “If you have information that links Hive or any other malicious cyber actors targeting U.S. critical infrastructure to a foreign government, send us your tip via our Tor tip line. You could be eligible for a reward.” This reportedly prompts Roskomnadzor to block access to the FBI and other U.S. government websites. ([\(18\) Rewards for Justice on Twitter](#); The Cyber Wire, 1-30-2023)

January 26, 2023 – The Treasury Department announces new sanctions that include the Chinese firm Spacety China, accused of providing satellite imagery to the Russian Wagner Group. The move is described as part of an effort to curtail Russia's combat capabilities in Ukraine. ([US Treasury Targets Chinese Company in Broader Russia Sanctions Push - Bloomberg](#))

January 27, 2023 – Team Cymru provides technical details on hacktivist group NoName057(16), concluding, among other things, that its back-end infrastructure is

hosted in Russia. ([A Blog with NoName \(team-cymru.com\)](#); Risky Biz News, 1-27-2023)

January 27, 2023 – DefenseScoop publishes an interview with Estonian Permanent Secretary of the Estonian Ministry of Defence Kusti Salm in which he registers uncertainty about the ultimate impact of drones on the conduct of modern combat, especially in terms of their performance against air defense. “In order to make definite conclusions of what has been the change — or what is the really the sort of critical impact on the battlefield — we need to get more [data] and we need to dig deeper into this,” Salm asserts. ([NATO allies 'don't have enough data' on impact of drones in Russia-Ukraine war: Estonian official | DefenseScoop](#))

January 27, 2023 – Roskomnadzor has restricted access CIA and FBI websites, the Russian news site *Kommersant* reports. Later reports indicate the State Department’s Rewards for Justice site has also been blocked for “spreading fakes about the Russian military and discrediting them,” according to Roskomnadzor. ([Роскомнадзор заблокировал сайты ЦРУ и ФБР - Новости - Телекоммуникации - Коммерсантъ \(kommersant.ru\)](#); [Russia blocks access to US 'Rewards for Justice,' FBI and CIA websites - The Record from Recorded Future News](#))

January 27, 2023 – According to the cybersecurity firm Radware, a botnet called Passion “was leveraged during the attacks on January 27th, targeting medical institutions in the USA, Portugal, Spain, Germany, Poland, Finland, Norway, Netherlands, and the United Kingdom as retaliation for sending tanks in support of Ukraine.” The firm adds that “Passion group, affiliated with Killnet and Anonymous Russia, recently began offering DDoS-as-a-Service to pro-Russian hacktivists.” ([Passion: A Russian Botnet \(radware.com\)](#))

January 28, 2023 – Russian Deputy Foreign Minister Oleg Syromolotov tells TASS the United States is “aggressively recruiting hackers, training the so-called IT Army of Ukraine, and uses ... [its] partners and controlled private companies to carry out cyberattacks against Russia's information infrastructure.” He describes U.S. activity as “openly moving towards the militarization of the information domain.” ([Russia knows US recruits hackers, trains Ukrainian IT-army — Deputy Foreign Minister - Russian Politics & Diplomacy - TASS](#))

January 29, 2023 – A military factory in Isfahan, Iran, comes under a drone attack. Shortly afterwards, an adviser to President Zelensky, Mikhaïlo Podolyak, tweets: “Explosive night in Iran - drone & missile production, oil refineries. 🇺🇦 did warn you.” The Tweet prompts the Iranian Foreign Ministry to summon Ukraine’s chargé d’affaires. The *Wall Street Journal* later reports that Israel was behind the strike; Israel does not immediately comment. ([\(19\) Михайло Подоляк on Twitter](#); [Iran summons Ukraine’s envoy over drone attack comments | Russia-Ukraine war News | Al Jazeera](#))



January 30, 2023 – The Department of Health and Human Services issues an Analyst Note reporting that Killnet “is actively targeting the health and public health sector.” ([202301301200 KillNet Analyst Note TLPCLEAR \(hhs.gov\)](#))

January 31, 2023 – Head of the SSSCIP Yurii Shchyhol authors a short item summarizing “vital lessons for the West” from the war in Ukraine. A key point, he writes, is the link between conventional and cyber operations. “One year on, it is no longer possible to separate cyberattacks from other aspects of Russian aggression.” ([Russia’s cyberwar against Ukraine offers vital lessons for the West - Atlantic Council](#))

January 31, 2023 – Estonia’s Foreign Intelligence Service (Välisluureamet) publishes its annual report for 2022. ♦ Among its main findings on cyber issues: “Russia uses cyberattacks to support its general goals in Ukraine: to break Ukrainian resistance, undermine the government’s image and disrupt the functioning of the state. Cyber espionage is likely the biggest threat stemming from cyberspace. ♦ Russia underestimated the resilience of Ukraine’s cyberspace and the help it receives from Western countries and cybersecurity companies. ♦ Threats posted on social media and cyberattacks continue as part of the influence operations against countries that actively support Ukraine, including Estonia.” ([WEB VLA ENG-raport 2023.pdf \(valisluureamet.ee\)](#))

January 31, 2023 – Chief of Space Operations Gen. Chance Saltzman, speaking to reporters at the Pentagon, describes how the Ukraine war has shown that the space and cyber domains are “inextricably linked” on the electronic battlefield. “Satellites in space are not useful if the linkages to them and the ground network that moves the information around that you get from satellites is not assured, is not capable, is not accessible. And so I think we’ve witnessed some cyber activity that has hurt satellite operations. And so I think it’s a reminder that we think about satellite operations, but if we’re not thinking about cyber protection of our ground networks, that we may have a backdoor, if you will, to negate satellite operations without [conducting direct] counter-satellite operations — that there’s other ways to attack these systems,” Saltzman said during a meeting with reporters at the Pentagon.”

Saltzman makes numerous additional comments, as recorded by DefenseScoop. For example, he notes that Starlink has been “huge” for Ukrainian communications, planning, and operations, showing the war’s reliance on commercial space technology. “And the other thing that I kind of learned as an adjunct to that is that proliferated constellations in low-Earth orbit for satellite communications [are] much harder to degrade. It’s a tougher problem, in this case for the Russians. And so proliferation of constellations, commercial augmentation support to the military — I think we have to recognize that there’s some lessons to be learned there.” ([Space Force chief concerned about ‘backdoor’ for attacking satellite communications | DefenseScoop](#))

January 31, 2023 – Defense News posts a fascinating item on the U.S. Army’s ability to offer Ukrainian counterparts remote maintenance and repair support for U.S.-supplied

weapons systems. The Army has greatly built up the capability since the early phases of the conflict and is already applying lessons to its thinking about the future. According to Lt. Gen. Christopher Mohan, deputy chief of Army Materiel Command: "If we don't use [the war] as a window into what future warfare looks like on a very lethal and highly distributed battlefield, we're foolish." ([US Army goes virtual to help Ukraine maintain weapons \(defensenews.com\)](#))

January 31, 2023 – The Insikt Group of Recorded Future publishes "Dark Covenant 2.0: Cybercrime, the Russian State, and the War in Ukraine," a report that "examines the unspoken connections between the Russian Federation, Cybercriminals, and self-described hackers in Russia and Eastern Europe." Among its conclusions, the report notes that the war has brought various "transformational changes" to "several cybercriminal industries," including "changes to the malware as-a-service (MaaS) and ransomware-as-a-service (RaaS) threat landscapes, a rise in Russian payment card fraud, shifts in cybercriminal targeting, changes in infrastructure and hosting, and more." ([Dark Covenant 2.0: Cybercrime, the Russian State, and the War in Ukraine \(recordedfuture.com\)](#))

January 31, 2023 – ESET publishes "APT Activity Report, T3 2022," which includes reporting on Sandworm and other activity relating to the war in Ukraine. ([eset apt activity report t32022.pdf \(welivesecurity.com\)](#))

January 31, 2023 – The nonprofit group FS-ISAC produces a report titled "The Evolution of DDoS: Return of the Hacktivists," which notes a 22% rise in DDoS attacks during 2022, much of it from the Ukraine war. ([EvolutionOfDDoS-ReturnOfTheHacktivists.pdf \(fsisac.com\)](#))

Late January 2023 – The SSSCIP of Ukraine publishes a report title "Another UAC-0010 Story," which describes "frequent" recent activity by the Russia-sponsored group also known as Gamaredon and Armageddon. ([19b0a96e-8c31-44bf-863e-cd3e0b651f22.pdf \(scpc.gov.ua\)](#))

February 2023 – Killnet launches a series of attacks this month targeting hospitals in more than 25 U.S. states, continuing a trend noted by cybersecurity researchers that is believed to have begun in November 2022. ([Pro-Russia hackers are increasingly targeting hospitals, researchers warn \(therecord.media\)](#))

February 2023 – Four Android Technology Marker reconnaissance robots are scheduled to take part in combat operations this month, according to Dmitry Rogozin, former head of Roscosmos (see January 26, 2023, entry). ([Robot "Marker" will be prepared for the destruction of NATO tanks - RIA Novosti, 26.01.2023](#))

February 1, 2023 – CERT-UA reports it has detected a web page mimicking the Ukrainian Foreign Ministry website. "In cooperation with CERT Polska and CSIRT MON (Republic of Poland), we detected several more phishing websites to mimic web pages of the Security Service of Ukraine and the Polish Police. In addition, it should

be noted that a similar fraudulent web page was spotted impersonating the mail portal of the Ministry of Defense of Ukraine back in June 2022. We track mentioned activity under UAC-0114, aka Winter Vivern.” ([CERT-UA](#))

SentinelLabs later publishes the results of an investigation into Winter Vivern that concludes its activities “are closely aligned with global objectives that support the interests of Belarus and Russia’s governments. The APT has targeted a variety of government organizations, and in a rare instance, a private telecommunication organization.” ([Winter Vivern | Uncovering a Wave of Global Espionage - SentinelOne](#))

February 1, 2023 – On or about this date, the CyberPeace Institute releases its Q4 report on the “Cyber Dimensions of the Armed Conflict in Ukraine.” Among other findings: “The CyberPeace Institute documented 249 cyber incidents against entities in Ukraine between January and December 2022. With 71 incidents impacting 16 sectors in Q4, there has been a 18.4% decrease in incidents compared to the previous quarter. This decrease is driven by a decline in substantiated incidents targeting Ukrainian entities by pro-Russian hacktivist collectives.” ([Cyber Dimensions Ukraine Q4 Report.pdf \(cyberpeaceinstitute.org\)](#))

February 1, 2023 – Palantir CEO Alex Karp claims his data analytics company is “responsible for most of the targeting in Ukraine.” ([Ukraine is using Palantir's software for 'targeting,' CEO says | Reuters](#))

February 2, 2023 – Oleksii Rznikov, Ukraine’s minister of defense, warns Russia may be mounting a major offensive. He also claims the number of troops recruited and sent to Ukraine is “much more” than the 300,000 Moscow previously announced. ([Ukraine war: Russia planning 24 February offensive, Ukrainian defence minister says - BBC News](#))

February 2, 2023 – Twitter posts the following tweet: “Starting February 9, we will no longer support free access to the Twitter API, both v2 and v1.1. A paid basic tier will be available instead 📖 European Union High Representative for Foreign Affairs Josep Borrell responds that this could undermine attempts to understand Russian disinformation operations. ([\(20\) Twitter Dev](#))

February 4, 2023 – The Armed Forces of Ukraine officially adopts the Delta battlefield management system, under development since 2016, as part of its network-centric warfare doctrine. ([Joker DPR and the Information War \(recordedfuture.com\)](#))

February 4, 2023 – The *Wall Street Journal* reports on China’s provision of restricted technology to Russia for its war in Ukraine. The underlying data comes from the Washington-based organization C4ADS, which tracks and aggregates publicly available information on transportation, communications, and finance relating to selected illicit, international transactions. ([China Aids Russia’s War in Ukraine, Trade Data Shows - WSJ](#); [About Us - C4ADS](#))

February 4, 2023 – State Department Ambassador-at-Large for cyber Nate Fick tweets: “My account has been hacked. Perils of the job...” He offers no details. ([\(20\) Nate Fick on Twitter](#))

February 6, 2023 – CERT-UA announces it has discovered a phishing campaign against Ukrainian entities that covertly installs the remote surveillance software Remcos from Breaking Security. The agency attributes the malware to UAC-0050. ([CERT-UA](#))

February 7, 2023 – Claudia Plattner, director General Information Systems at the European Central Bank, is announced as the new president of the German Federal Office for Information Security (BSI) as of 1 July 2023. She replaces Arne Schönbohm, who lost his position after accusations of being connected to Russian intelligence. ([ECB's Director General Information Systems to lead German Federal Office for Information Security \(BSI\) \(europa.eu\)](#))

February 7, 2023 – The European External Action Service's (EEAS) Stratcom division publishes a report on “Foreign Information Manipulation and Interference Threats” that it bills as a “first of its kind.” Findings include that the invasion of Ukraine is a dominant theme of Russia's “FIMI” activity, that Moscow uses diplomatic channels regularly to enable these operations, that they often involve increasingly sophisticated impersonation techniques (pretending to be trusted international organizations), and that Russia and China both aim mainly to shift blame and distort the narrative. ([EEAS-ThreatReport-February2023-02.pdf \(euvdisinfo.eu\)](#))

February 7, 2023 – Moldova's prime minister, Natalia Gavriluța, tells Euronews: “We are seeing elements of hybrid war” coming from Russia. “We are seeing cyberattacks. We've had the biggest cyberattacks in 2022 in the history of our country, and we are seeing bomb threats. A lot of the situation in Moldova will depend on the evolution of the war in Ukraine.” ([Russia conducting 'hybrid war' in Moldova with protests and cyber attacks: Prime Minister | Euronews](#))

February 8, 2023 – SpaceX President Gwynne Shotwell says at an FAA conference that the company's Starlink equipment was “never meant to be weaponized.” “We know the military is using them for comms, and that's OK. But our intent was never to have them use it for offensive purposes.” She adds: “There are things that we can do to limit their ability to do that ... There are things that we can do, and have done.” She offers no details.

*Politico* reports that Russian Telegram channels “appeared to light up with glee over the news,” while Zelensky adviser Mykhailo Podolyak “tweeted that Musk would have to decide whether he was with Ukraine's right to freedom or Russia's will to try to illegally seize sovereign territory. ‘#SpaceX (Starlink) & Mrs. #Shotwell should choose a specific option.’”

It's not entirely clear whether Shotwell was claiming that Starlink itself was never meant to be weaponized or whether SpaceX never wanted the Ukrainians specifically to use it offensively. But Defense One points out the company has been



involved with the U.S. Army in developing battlefield applications for Starlink. ([Ukraine war: Elon Musk's SpaceX firm bars Kyiv from using Starlink tech for drone control - BBC News](#); [Musk Switches Off Ukraine's Starlink for Drones \(foreignpolicy.com\)](#); [SpaceX admits blocking Ukrainian troops from using satellite technology - CNNPolitics](#); [Decrying Starlink's 'Weaponization,' SpaceX Cuts Support for Ukrainian Military - Defense One](#))

February 9, 2023 – The U.K. and U.S. governments slap sanctions on seven high-profile Russian ransomware offenders as part of what the British call “the first wave of new coordinated action against international cyber crime” in tandem with the United States. The seven are Vitaliy Kovalev, Valery Sedletski, Valentin Karyagin, Maksim Mikhailov, Dmitry Pleshevskiy, Mikhail Iskritskiy, and Ivan Vakhromeyev.

The U.K. announcement continues: “Ransomware groups known as Conti, Wizard Spider, UNC1878, Gold Blackburn, Trickman and Trickbot have been responsible for the development and deployment of: Trickbot, Anchor, BazarLoader, BazarBackdoor as well as the ransomware strains Conti and Diabol. They are also involved in the deployment of Ryuk ransomware.”

“Conti was one of the first cyber crime groups to back Russia’s war in Ukraine, voicing their support for the Kremlin within 24 hours of the invasion. Although the ransomware group responsible for Conti disbanded in May 2022, reporting suggests members of the group continue to be involved in some of the most notorious new ransomware strains that dominate and threaten UK security.” ([UK cracks down on ransomware actors - GOV.UK \(www.gov.uk\)](#))

February 9, 2023 – A Radware Cybersecurity Advisory reports: “Infinity Team, a collaboration between Killnet and Deanon Club, has established its own forum and marketplace called Infinity. The forum offers advertisement spaces, paid status for those who want to perform business on the forum, and is currently offering a variety of hacking resources and services through its hack shop, including DDoS services.” ([Advisory-Infinity-Forum-022023.pdf.aspx \(radware.com\)](#))

February 12, 2023 – The London *Telegraph* reports that Killnet was behind a recent disruption of aid efforts for survivors of the earthquake in Turkey and Syria. The hacker group claims credit for the attack, announcing it on Telegram. NATO Special Operations Headquarters in Belgium, the Strategic Airlift Capability (a multinational initiative), and other organizations were reportedly affected, albeit briefly. The *Telegraph* reports that a SAC C-17 pilot said to be delivering supplies to Incirlik Air Base in Turkey learned from a SAC manager that NATO’s NR (NATO Restricted) network had experienced a DDoS attack. ([Russian Killnet hackers disrupt Nato's Turkey-Syria earthquake relief \(telegraph.co.uk\)](#))

February 13, 2023 – CERT-UA reports on a spearphishing operation by an entity identified as UAC-0096, which sent emails purportedly on behalf of the Staff of the National Security and Defense Council of Ukraine. ([CERT-UA](#))

February 13, 2023 – Russian officials announce the creation of a system designed to search the internet for illegal content, such as anti-war activity and “LGBT propaganda.” The “Oculus” system will be able to analyze more than 200,000 images per day, according to the Interfax news agency. ([Russian system to scan internet for undesired content and dissent | Reuters](#))

February 14, 2023 – The growing use of Starlink by Ukrainian forces in countering Russia’s invasion is the topic of a piece by C4ISRNET, which maintains that the trend is speeding up the development of drone warfare. ([Musk’s Starlink satellites accelerating development of drone warfare \(c4isrnet.com\)](#))

February 15, 2023 – NATO announces that 16 of its members have launched a new initiative to speed up and streamline information sharing from space. The Alliance Persistent Surveillance from Space (APSS) will consist of satellites and other space technology, national and commercial, to expand alliance cooperation and cut the costs of doing so. ([NATO - News: 16 Allies, Finland and Sweden launch largest space project in NATO’s history, 15-Feb.-2023](#))

February 15, 2023 – A *Financial Times* article spotlights the work of Christo Grozev, an investigative reporter with Bellingcat, in part because of his (and Bellingcat’s) extensive use of OSINT (open-source intelligence). The article notes that “one overlooked feature of the Ukrainian war is that it has accelerated the cause of forensic digital journalism in an extraordinary way. The reason Grozev is on the Kremlin’s blacklist is because Osint is creating once-unimaginable levels of transparency.” An example is the Bulgarian-born journalist’s success in uncovering the identities of a remote Russian missile programming team (see October 24, 2022, entry). “In line with Osint ideals, Grozev explained that he had identified the unit by cross-checking databases on food deliveries, cell phones, Russian army records and geolocated photographs.” “The result is a conflict that is arguably the most transparent in history.” ([The keyboard warriors on Ukraine’s digital front line | Financial Times \(ft.com\)](#))

February 15, 2023 – The Belarusian Cyber-Partisans, hackers opposed to President Alexander Lukashenko, dumped 335 GB of files and emails from Roskomnadzor’s General Radio Frequency Centre (GRFC) division. The group provided the material to the site Distributed Denial of Secrets. The files give insights into Roskomnadzor’s censorship practices, according to *Süddeutsche Zeitung*. ([Huge data dump from Russia’s censorship agency posted online - Cyber Security Connect](#))

February 15, 2023 – At the first conference on responsible use of AI in the military (REAIM) in Amsterdam, Palantir CEO Alex Karp argues that exploiting artificial intelligence on the battlefield has moved from a “highly erudite ethics discussion” to a requirement to be able to “identify the right technology and implement it.” He says the West needs to grasp that “this lesson is completely understood by China and Russia.” He adds that there should be an “architecture that allows transparency on the data sources” which “should be mandated by law [and] more importantly ... by

purchasing regulation.” ([Ukraine war shows urgency of military AI, Palantir CEO says | Reuters](#))

February 15, 2023 – CISA Director Jen Easterly comments on the Ukraine conflict, noting the general “surprise” at the lack of “significant attacks” by pro-Moscow groups outside of Ukraine and attributing this to CISA’s “Shields Up” awareness campaign, Russia’s overconfidence, and its concern about escalation.

At the same time, Dmitri Alperovitch tells the *Washington Post* there have been more attacks than people realize. “The Ukrainians have done an amazing job keeping much of it under wraps,” he said. “Not all the attacks have been successful, but even those that have been successful have been in many cases kept under wraps, and the Ukrainians in general obviously do not want to give Russia a propaganda victory by admitting that some of their attacks had succeeded.”

In the same *Post* column, Mark Savchuk of the Ukrainian Volunteer Journalists Initiative makes the point that while the current conflict has lessons for the future, there are some elements of this experience that will not necessarily translate: namely, that neither Russia nor Ukraine integrate weapons with networks, unlike countries such as China and the U.S. If those two powers, for example, go to war, “That will present unique opportunities to cyber for disruption and potentially even disabling of critical offensive capabilities, at least in the opening stages of conflict. And maybe even throughout.” ([What we've learned from a year of Russian cyberattacks in Ukraine - The Washington Post](#))

February 16, 2023 – This week, Yevgenii Prigozhin, head of the Wagner Group, tells reporters that he not only financed but “invented ... created” the infamous Internet Research Agency, credited/blamed for interfering with prior U.S. elections. “I ran it for a long time,” Prigozhin says. A *Washington Post* article notes that the impact of the IRA’s operations is hard to measure, while cyber expert Thomas Rid warns that any claim of meaningful influence by the likes of Prigozhin should be taken with a grain of salt. “The whole narrative and collective conversation around disinformation is occupying such a big space that it is more impactful than the actual operation being carried out.” ([Wagner mercenary chief says he is also behind Russian information war - The Washington Post](#))

February 16, 2023 – The *Wall Street Journal* reports on the extraordinary impact of smartphones in the war in Ukraine, making it “the most intensively documented in history, changing the shape of the conflict and transforming the world’s understanding of it.” They have been, and continue to be, used to monitor developments on the battlefield, identify military targets, guide drones, assess damage, and record atrocities. Sometimes they are exploited by the warring sides unbeknownst to users – for instance, by locking onto the phones’ sensors that can pinpoint places and times and using that data to launch strikes.

“The digital documentation provided by smartphones is already overwhelming,” the article notes. “Mnemonic, a Berlin-based nonprofit documenting human-rights abuses in Ukraine, said it has collected 2.8 million digital records in less than a year.” These records, including utterly unfiltered images and sounds

logged via the likes of Facebook, Instagram, TikTok, and especially Telegram, are already being combed through for evidence of war crimes. ([Smartphones Are Changing the War in Ukraine - WSJ](#))

February 16, 2023 – A former USG and current private sector cyber expert, Joe Słowik, posts an analysis of Russian cyber operations in Ukraine along with lessons to be gained. He points out that Russia's generally unexpected lack of a coherent cyber strategy tied to its kinetic campaign should not come as a surprise given its difficulties on the battlefield. That factor may partially explain their resort to "war crimes and terror campaigns" which go after "more permissive targets." He comments that "the scope and reach of non-state organizations in cyber operations is vast and – arguably – insurmountable" and thinking that a Western government could achieve success without the help of key private entities "would be delusional," although the "manner" in which commercial firms might play a part remains "unexplored." He ends by saying that before dismissing Russian efforts as simple incompetence, "we should be humble in understanding no one has yet figured out precisely how and where 'cyber' fits into traditional military operations." ([What Have We Learned? – Stranded on Pylos](#))

February 16, 2023 – Google's Threat Analysis Group, along with Mandiant and Trust & Safety, produce a one-year assessment, "Fog of war: How the Ukraine Conflict Transformed the Cyber Threat Landscape." Its main "observations" are that Moscow-backed actors have "engaged in an aggressive, multi-pronged effort to gain a decisive wartime advantage in cyberspace, often with mixed results;" the Kremlin has used "the full spectrum of information operations — from overt state-backed media to covert platforms and accounts — to shape public perception of the war;" and Russia's invasion has "triggered a notable shift in the Eastern European cybercriminal ecosystem that will likely have long term implications for both coordination between criminal groups and the scale of cybercrime worldwide." ([google fog of war research report.pdf](#))

February 16, 2023 – Aspen Digital releases a report on international cyber assistance efforts to Ukraine and offers lessons. "[T]his paper seeks to define cyber defense assistance, outline its primary component parts, and identify key lessons learned that can help inform how such assistance can be provided in future geopolitical conflicts. It makes the case that an effective national security toolkit requires the ability to deliver cyber defense assistance to allies." ([CDAC Paper \(aspeninstitute.org\)](#))

February 17, 2023 – At the Munich Cyber Security Conference, Mauro Vignati, adviser to the International Committee of the Red Cross on the digital technologies of warfare, discusses the question of applying combatant status to hacktivists during time of war. "Encouraging civilian participation in cyber activities during armed conflict could undermine the protection of civilians who must be spared from the effects of armed conflict." He says the ICRC "strongly recommends states to reverse the trend



of civilianization of the digital battlefield.” (Recorded Future cited in The CyberWire, 2-21-2023)

February 17, 2023 – A multi-nation exercise called Defence Cyber Marvel 2 (DCM2) wraps up today in Estonia. It was organized by the British Army whose own military intelligence team places first in a contest to simulate Russian disruptive tactics from the beginning stages of the war in Ukraine. ([UK military intelligence team wins Western Europe’s ‘largest cyber warfare exercise’ held in Estonia \(therecord.media\)](#))

February 18, 2023 – Tony Blinken says that the U.S. government has spoken with Elon Musk recently about the deployment of Starlink devices to Ukraine, but he declines to offer details. ([Elon Musk, U.S. discussed Starlink in Ukraine, Blinken says | Reuters](#))

February 20, 2023 – The Main Radio Frequency Center (GRCHC), a part of Roskomnadzor, announces the planned launch in the second half of 2023 of the “Boar” (*Vepr*) system, which is designed to scour the Internet for material deemed to be potentially threatening. “The development of the Vepr information system has been underway since 2022,” the GRCHC says, with the first modules of the system currently undergoing testing. ([Систему "Вепрь" для выявления угроз в интернете запустят во второй половине 2023 года \(tass.ru\)](#))

February 21, 2023 – The IT Army of Ukraine claims credit for a DDoS attack that temporarily takes Vladimir Putin’s annual state of Russia speech offline. A group said to have ties to Alexei Navalny also participated, according to reports. ([Vladimir Putin speech broadcast interrupted by 'DDoS attacks' \(techmonitor.ai\)](#))

February 21, 2023 – The reported push to utilize “killer robots” in combat is explored in the academic outlet *The Conversation*. ([War in Ukraine accelerates global drive toward killer robots \(theconversation.com\)](#))

February 21, 2023 – Department of Homeland Security Under Secretary for Policy Robert Silvers tells Politico: “Overall, Ukraine has been able to defend itself, its cybersecurity and its critical networks, much more effectively than I think even the optimists thought that it might ... And our lesson taken away from that is we should be looking for opportunities to work with international partners much more intensively across the board.”

The article goes on to say: “Since before Russian tanks crossed the border, Silvers said, the Department has been working ‘at a high velocity and intensity’ to support Ukraine’s computer emergency response team. Those engagements include daily threat exchanges, joint malware analyses and an ongoing program that brings Ukrainian operators to Idaho National Labs, where U.S. officials train them how to defend industrial control systems.” ([Inspired by Kyiv, DHS eyes new foreign partnerships - POLITICO](#))

February 21, 2023 – A media report relates that Come Back Alive, said to be Ukraine's largest charitable foundation, has started a fundraising campaign hoping to raise \$1.3 million in support of Ukraine's cyber forces. The funds will be used to buy "technology and equipment that will help Ukraine's cyber forces conduct digital operations that could impede Russia's advances on the real battlefield," the article notes. Come Back Alive has already raised more than \$200,000 on behalf of Ukrainian cyber efforts. ([Ukraine's largest charity wants to raise \\$1.3 million for 'cyber offensive' \(therecord.media\)](#))

February 21, 2023 – Ukrainians involved in the country's cyber operations are reported to see their approach as a model for other states. A *Newsweek* article discusses the idea but adds: "But there are also serious questions about this new way of war that Ukraine is waging. Critics argue that it blurs important legal lines between combatants and civilians, including foreigners; ignores norms of international behavior in cyberspace by attacking civilian targets; potentially disrupts other intelligence operations; risks dragging other countries into the war by striking Russian allies such as Belarus, and may give the Russians an excuse to escalate the conflict by striking at pro-Ukrainian hackers based in neighboring third countries. Above all, they say, Ukraine's approach may work well for defense, but could prove dangerously counterproductive on offense." ([Ukraine's Volunteer Cyber Army Could Be Blueprint for the World: Experts \(newsweek.com\)](#))

February 2023 – The National Endowment for Democracy (NED) publishes a report called *Shielding Democracy* covering Russian disinformation on Ukraine and civil society responses. According to public opinion polls from late 2022, Kremlin efforts have not taken hold in Ukraine or Europe. "The research identified three advantages—deep preparation, open networks of cooperation, and active utilization of new technology—that have allowed civil society organizations and governments in Ukraine and Central and Eastern Europe to build trust and tell Ukraine's story, unite Ukrainians and their allies, and ensure resilience in the face of authoritarian disinformation campaigns," the document reads. ([NED FORUM-Shielding-Democracy.pdf](#))

February 22, 2023 – The Atlantic Council releases *Undermining Ukraine: How the Kremlin Employs Information Operations to Erode Global Confidence in Ukraine*. The 37-page report is based on daily monitoring by the Council's Digital Forensic Research Lab and concludes that while Russia's efforts cannot be seen as better than "spotty," the various effects of its information operations relating to the Ukraine war "will have much longer shelf life, well beyond the confines of the current conflict." ([Undermining-Ukraine-Final.pdf \(atlanticcouncil.org\)](#); [Inside Russia's Year of Ukraine Propaganda | Time](#))

February 22, 2023 – *The Washington Post* reports that a new Twitter paid verification system is being used increasingly by accounts advancing pro-Moscow propaganda, citing research by the firm Reset. The blue-check verifications can be bought by anonymous accounts and Reset has found a dozen that were set up in the early

stages of the Ukraine war but have only recently become paid subscribers – since Elon Musk introduced a new “pay-to-play model,” according to the *Post*. ([Russian propagandists get Twitter verification two years in Ukraine war - The Washington Post](#))

February 22, 2023 – *Wired* recounts Ukraine’s experiences as the target of an unprecedented number of cyberattacks – mostly malware – in 2022. An ESET researcher calls it “the most intense use of wipers in all computer history.” Since early 2022, the article notes, Russian strategy has shifted from “masterpieces of malevolent code that required months to create and deploy” to “quick, dirty, relentless, repeated, and relatively simple acts of sabotage.” ([Ukraine Suffered More Wiper Malware in 2022 Than Anywhere, Ever | WIRED](#))

February 22, 2023 – *Breaking Defense* publishes an item by Mark Cancian of CSIS revisiting five predictions made by experts a year ago about the war in Ukraine. On the role of cyber, he concludes it has not been a “game-changer” and in fact has had “no discernible effect on military operations.” A key reason is that cyber weapons are “generally one-time use” which means that victims of an attack are almost always able to fix the vulnerability. The overall lessons are “that effective defenses are possible, and the scariest cyber scenarios are unlikely to occur.” ([A year into Ukraine, looking back at 5 prewar predictions - Breaking Defense](#))

February 23, 2023 – In an alert, CISA “assesses that the United States and European nations may experience disruptive and defacement attacks against websites in an attempt to sow chaos and societal discord on February 24, 2023, the anniversary of Russia’s 2022 invasion of Ukraine.” ([CISA Urges Increased Vigilance One Year After Russia's Invasion of Ukraine | CISA](#))

February 23, 2023 – New data released today from Meta leads the company’s head of security policy to describe Russia’s influence operations methods as “smash-and-grab” and a “‘throw the spaghetti against the wall to see what sticks’ approach.” In the words of one reporter: “Instead of slowly building up an audience, influence operatives are now flooding the platform with low-quality accounts hoping some evaded Meta’s detection.” Speaking to reporters, Meta’s president of global affairs Sir Nick Clegg notes further that the use of fake accounts is not new but the sharp increase in the practice seems to signify a shift in Russian strategy, the purpose of which is not entirely clear. ([Russia's information war against Ukraine went stealth after Meta crackdown | CyberScoop; Russian 'smash-and-grab' social media operation on Facebook and Instagram attempting to influence Ukraine war - Meta report | Science & Tech News | Sky News](#))

Graphika today publishes a report called “How to Lose Influence and Alienate People” and produced in tandem with Meta that analyses the impact of restrictions placed by social media platforms on the posting activities of Russian state-controlled media. The authors find that impact to be “significant” but also raise questions about when and how to use “such powerful tools.” ([How to Lose Influence and Alienate People \(graphika.com\)](#))

February 23, 2023 – CERT-UA announces it has uncovered an attack on several Ukrainian official websites at the central and local levels. The agency says the breaches used backdoors inserted as early as December 2021. The hackers (tracked as UAC-0056, Ember Bear, or Lorec53) deployed CredPump, HoaxPen, and HoaxApe backdoors as well as the GOST and Ngrok tools. ([Detected cyberattack on a number of Ukrainian government information resources \(cip.gov.ua\)](#); [Ukraine says Russian hackers backdoored govt websites in 2021 \(bleepingcomputer.com\)](#))

February 23, 2023 – TRM issues a report, “The First Crypto War?” “As the war marks its grim first anniversary, TRM Labs has focused its analysis on the state of the illicit crypto ecosystem over the past year. This report discusses how cybercriminals have adjusted their organization and tactics to adapt to the ongoing financial, political and logistical disruptions facing Europe and the wider world.” ([TextDocumentTemplate \(website-files.com\)](#))

February 24, 2023 – Treasury’s OFAC imposes a series of sanctions on Russian entities, including two Moscow-based concerns involved in cyber activity. ODay Technologies, a cybersecurity consulting firm, and Forward Systems, R&DC, specializing in computer programming and information technology, have both provided material support to Russian intelligence. ([Targeting Key Sectors, Evasion Efforts, and Military Supplies, Treasury Expands and Intensifies Sanctions Against Russia | U.S. Department of the Treasury](#))

February 24, 2023 – (Date approx.) A public report issued by Dutch intelligence includes a section on Russian cyber activities in and around Ukraine. It reaffirms that Russian intelligence and security services have conducted “large-scale digital espionage, sabotage and influence operations against Ukraine and NATO allies” and that while many of them were blunted by Ukrainian and Western defenses, “[t]he tempo of Russian cyber operations is high and many of their attempts have not yet been made public.” Although “the Russian Federation struggles to synchronise cyber operations with other military operations, such as air strikes .... Ukraine and Western defenders must remain vigilant in the face of the constant and extreme pressure.” ([Dutch-intelligence-report-February-2023](#))

February 24, 2023 – The Canadian Centre for Cyber Security urges Canadian organizations “to be vigilant and prepared for malicious cyber activity following the one-year mark of Russia’s full-scale invasion of Ukraine.” ([Canadian Centre for Cyber Security](#))

February 24, 2023 – A media report on Russian cybercrime since the invasion of Ukraine notes that after an initial dip in the number of attacks a number of underground organizations have begun to ramp up again. This includes individuals who left Russia to avoid the draft, according to Arctic Wolf. ([UA A year of cyber warfare \(axios.com\)](#))



February 24, 2023 – Another anniversary piece goes into detail on the past year of Russian cyber operations relating to Ukraine. Based on numerous interviews with experts, CyberScoop describes the scope of cyber activities and notes that the defensive aspects have been “unprecedented.” ([A year after Russia's invasion, the scope of cyberwar in Ukraine comes into focus | CyberScoop](#))

February 24, 2023 – A report by Recorded Future describes how the war in Ukraine has disrupted the “cybercriminal ecosystem” in Russia, Ukraine, and Belarus. Political disagreements and the IT brain drain have been major factors. In addition, “[i]nternational arrests, seizures, and disruptive actions have destabilized the business model associated with commodified cybercrime.” ([Russia's War Against Ukraine Disrupts the Cybercriminal Ecosystem \(recordedfuture.com\)](#))

February 25, 2023 – The *Washington Post* runs an overview of Ukraine’s cyber experience of the past year noting, among other things, various ways Ukraine was able to fend off Russian attacks. They include the use of physical tokens as secondary authentication and Russia’s reuse of code from prior hacks that security software was able to detect. ([Cyberattacks on Ukraine helped better cybersecurity in U.S. - The Washington Post](#))

February 25, 2023 – A former member of Group-IB who fled to Poland describes some of his activities as an analyst of open data for the nominally private company. Group-IB is said to be a well-known provider of information security tools. The former analyst estimates that the federal security services are at least aware of 99% of Russian hacker activity. (The quoted phrase in Russian is “Полагаю, что 99,9% находятся в их поле зрения ...,” which literally translates as “I believe that 99% are within their field of view,” but the headline of the interview says, in quotation marks, “99% российских хакеров контролирует ФСБ,” which translates as “the FSB controls 99% of Russian hackers.”) ([«99% российских хакеров контролирует ФСБ» \(novayagazeta.eu\)](#))

February 25, 2023 – A Russian hacking group, Zarya (reported to be linked to Killnet), shows screenshots of their alleged breach of a Canadian gas pipeline company network to an FSB officer. The briefing is later leaked to the Discord gaming channel, which included a variety of documentation about the war in Ukraine. The material appears to indicate the group was able to change valve pressure, disable alarms, and even shut down the pipeline, according to a write-up by Zero Day, which examined the leaked briefing. ([Leaked Pentagon Document Claims Russian Hacktivists Breached Canadian Gas Pipeline Company \(google.com\)](#))

February 26, 2023 – An Australian media report discusses the “almost unprecedented” impact of Russian rocket strikes on Ukraine’s energy and communications infrastructure. The article quotes the director of Melbourne’s IP Observatory: “It would appear ... that the increased bombings and attacks on civilian infrastructure [since October 2022] is really starting to have a major impact on the Ukrainian

experience of basic things like connection to the internet." ([The battle to keep Ukraine connected to the internet amid Russian missile attacks - ABC News](#))

February 27, 2023 – Ukrainian senior cyber official Victor Zhora gives a lengthy interview to CyberScoop. Among other comments, he says that Russian cyberattacks shouldn't be underestimated but they have not been nearly as destructive as kinetic attacks and have mainly been used for psychological operations or espionage, targeting civilians to a large extent because the Russian military has been ineffective against Ukraine's armed forces. He speculates that attacks on Ukraine's allies are "a kind of revenge" and they only continue because the military officers conducting them have to "report to their generals that they are doing something." (['A year of cyberwar' with Russia: An inside look from a top Ukrainian cybersecurity official | CyberScoop](#))

Late February 2023 – The Pentagon includes Altius 600M drones in its \$2 billion aid package to Ukraine, according to Palmer Luckey, founder of the firm Anduril that makes the aircraft. ([Anduril autonomous drones to aid Ukraine - Australian Defence Magazine](#))

Late February 2023 – James Rubin, a coordinator for the State Department's Global Engagement Center, which aims to "expose and counter" foreign propaganda and disinformation, tells European audiences that China has sunk billions of dollars into "pernicious" disinformation campaigns that support Russia's position in Ukraine. He laments that the U.S. and the West have been "slow to respond." ([China spends billions on pro-Russia disinformation, US special envoy says | China | The Guardian](#))

February 28, 2023 – Cardiff University publishes a lengthy analysis of "Ghostwriter" (UNC1151), which has been active since at least 2016 and believed to have the support of either Belarus or Russia, or both. "This report synthesizes publicly available open-source data to map the evolution of the 'Ghostwriter campaign', tracking and tracing how it has: (1) blended information manipulation with hacking; (2) targeted a number of countries; (3) operated successfully across a range of platforms; and (4) evolved and adapted over time." ([Ghostwriter-Report-Final.pdf \(cardiff.ac.uk\)](#))

February 28, 2023 – The German Regional Police and Ukrainian National Police, with support from Europol, the Dutch Police, and the FBI, "targeted suspected core members of the criminal group responsible for carrying out large-scale cyberattacks with the DoppelPaymer ransomware," according to a Europol statement. Locations where equipment was seized included Kyiv and Kharkiv. ([Germany and Ukraine hit two high-value ransomware targets | Europol \(europa.eu\)](#))

February 28, 2023 – A media report details the flight of tech workers from Belarus, "Europe's last dictatorship," since 2020. Government statistics from destination countries indicate about 120,000 Belarusians have left – about 20,000 of them (by June 2022) coming from the IT sphere, which had an estimated total workforce of

60,000 to 100,000 people. ([Russia's Ukraine invasion forced Belarusian tech workers abroad - Rest of World](#))

February 28, 2023 – Poland's online tax filing system is hit by a DDoS attack. A Polish official accuses Russia of responsibility. The Russian embassy in Warsaw denies it. ([Poland says Russian hackers attacked tax website | Reuters](#))

February 28, 2023 – A piece in *Foreign Affairs* touts the experience of the Ukraine war in arguing that “innovation power” has become a defining force in geopolitics. ([Eric Schmidt: Why Technology Will Define the Future of Geopolitics \(foreignaffairs.com\)](#); [China spends billions on pro-Russia disinformation, US special envoy says | Russian internet speeds drop on hardware shortage | Belgium's cyber security agency links China to attack on MP \(substack.com\)](#))

February 28, 2023 – A Russian court fines the Wikimedia Foundation 2 million rubles (about \$27,000) for failing to delete "misinformation" about the war in Ukraine. It is Wikipedia's third fine the invasion. ([Russian court fines Wikipedia over military 'misinformation' | Reuters](#); [Risky Biz News: White House unveils National Cybersecurity Strategy \(substack.com\)](#))

March 2023 – A classified U.S. intelligence report prepared this month and later obtained by the *Washington Post* discusses Russian testing of its Tobol electronic warfare system against Starlink terminals operating in eastern Ukraine. The *Post* publishes its report in mid-April. ([Russia unveils secretive weapon to target SpaceX's Starlink in Ukraine - The Washington Post](#))

March 1, 2023 – The Record writes about “A year of wipers” – describing the activities of the Sandworm group which Ukraine's SSSCIP estimates has conducted at least 30 cyberattacks in the country since Russia's invasion. Most of the hits have been wiper attacks. ([A year of wipers: How the Kremlin-backed Sandworm has attacked Ukraine during the war \(therecord.media\)](#))

March 1, 2023 – A Polish legal scholar, Joanna Kulesza, publishes an item in *Directions*, a blog by EU Cyber Direct, looking at the cyber component of the Ukraine war and how international law is being applied to it. “Russia committed a grave violation of international law when it invaded Ukraine one year ago. Russia and Ukraine are at war, but are they also at cyber war? We have seamlessly passed the much-debated Article 51 UNC threshold and moved into a cyber warzone, where shelling of Ukrainian towns and villages is accompanied by cyberattacks on its allies' critical infrastructure. How does this impact the application of international law in cyberspace?” ([Ukraine Cyber War One Year On: An International Law Case Study | directions blog](#))

March 1-2, 2023 – Part of the timeline of the dissemination of classified records on the Ukraine war and other topics obtained by Airman 1st Class Jack Teixeira is as follows (according to a tweet from Aric Toler of Bellingcat): “30+ leaked documents

were shared on the WowMao Discord server on March 1st and 2nd[;] 10 files were reposted [sic] on a Minecraft Map Discord server on March 4th[.] On April 5th, 3 of these files were posted on 4chan and 5 (incl. a doctored document) on Russian Telegram channels.” ([\(19\) Aric Toler on Twitter](#))

Early March 2023 – BlackBerry researchers detect new activity by Nobelium (APT29, Cozy Bear) aimed at members of the European Union, specifically “diplomatic entities and systems transmitting sensitive information about the region's politics, aiding Ukrainian citizens fleeing the country, and providing help to the government of Ukraine.” A Blackberry report adds: “Although its phishing campaigns aren’t very sophisticated, APT29 is notorious for its agility once it is inside a target’s network. Its operators are known to be stealthy, extremely patient, and skilled in utilizing innovative intrusion techniques that abuse Microsoft technologies and services.” ([NOBELIUM Uses Poland's Ambassador's Visit to the U.S. to Target EU Governments Assisting Ukraine \(blackberry.com\)](#))

Early March 2023 – Staff of the Russian Presidential Administration are given till April 1 to replace any iPhones they are currently using with a different device. First Deputy Head Sergey Kiriienko, in charge of domestic policy, gives the instruction for security reasons, according to sources cited by the news outlet Kommersant. The sources believe iPhones are more susceptible to breaches by Western specialists. ([Unwanted communications – Newspaper Kommersant No 46 \(7491\) dated 20.03.2023](#))

March 2, 2023 – The White House rolls out its new “National Cybersecurity Strategy,” which only mentions Ukraine in passing but reportedly takes several lessons from the conflict there, including the need to promote collaboration and partnerships with allies. ([National-Cybersecurity-Strategy-2023.pdf \(whitehouse.gov\)](#); [Biden vows to wield ‘all instruments’ in fighting cyberthreats \(defensenews.com\)](#))

March 2, 2023 – According to the International Press Institute, “On 2 March 2023, Halychyna FM, a highly popular radio station broadcasting in Western Ukraine, was targeted in a cyber attack likely initiated by Russian hackers. On its Facebook page, Halychyna FM posted screenshots from a pro-Kremlin Telegram channel known as The People’s Cyber Army (‘Narodnaya Cyber-Armiya’, in Russian), which on 1 March asked its over 6000 followers to attack the Ukrainian radio station. As a result, the radio’s website was inaccessible for an unspecified amount of time, with access fully restored by 2 March.” ([Radio Halychyna cyber-attacked following appeal by Russian hacker group - International Press Institute \(ipi.media\)](#))

March 2, 2023 – Russian Telegram channels report that DJI drones are almost entirely blocked for purchases by customers in the Russian Federation. ([\(20\) Faine Greenwood on Twitter](#); [New report: ASPI’s Critical Technology Tracker - The global race for future power | New US cybersecurity strategy assigns responsibility to tech firms | Poland blames Russian hackers for cyberattack \(substack.com\)](#))



March 2, 2023 – The use of OSINT to track and target Russian forces by a Ukrainian private company, Molnar, is detailed in a piece on ForeignPolicy.com. The firm takes social media posts, for example by Russian soldiers, identifies their likely location through Internet searches and other open sources, then passes the data on to Ukrainian intelligence. This use of OSINT is not an entirely novel concept, “[b]ut what is new in Ukraine is how these techniques are being reverse-engineered: not to retrospectively expose atrocities and malfeasance but to proactively kill enemy forces and destroy enemy hardware on the battlefield itself.” The practice “has prompted significant changes to the way operational security (OPSEC) is handled by militaries,” and has had occasionally unintended effects such as limiting journalistic coverage of the conflict. ([A Private Company Is Using Social Media to Track Down Russian Soldiers \(foreignpolicy.com\)](https://foreignpolicy.com/article/a-private-company-is-using-social-media-to-track-down-russian-soldiers/2023/03/02/))

March 2, 2023 – Recorded Future publishes a 2022 annual threat analysis report, prepared by the Insikt Group, which begins: “The physical conflict in Ukraine, and the effects it has had on the cyber threat landscape throughout 2022, frames our discussion of significant cyber threat events and geopolitical trends that occurred in 2022 and underscores the increased convergence of the cyber and geopolitical threat landscape. Before and throughout the physical invasion, Recorded Future has observed increased instances of distributed denial-of-service (DDoS) attacks, hacktivist activity, and the widespread deployment of wiper malware.” ([2022 Annual Report \(recordedfuture.com\)](https://recordedfuture.com/2022-annual-report/))

March 3, 2023 – Corvus Insurance offers “observations” on cyberwarfare in Ukraine, summarizing various expert conclusions and adding one or two other points, such as characterizing Western preconceptions about Russian cyber doctrine as suffering from “a degree of egocentrism” and noting that cyber criminals will undoubtedly reap benefits from Russia’s continued development of “tools to attack Ukraine’s networks.” ([Cyberwarfare in Ukraine: One Year of Observations \(corvusinsurance.com\)](https://corvusinsurance.com/cyberwarfare-in-ukraine-one-year-of-observations/))

March 7, 2023 – Russia’s U.N. cybersecurity representative, Irina Tyazhlova, accuses the West of using Ukraine as a “testing ground” for cyberattacks and has been seeking to undermine Russia with “massive cyberattacks” since the “special operation” began in 2022. ([Russian diplomat blames West for recruiting hackers for operations against Moscow - Russia - TASS](https://tass.com/ukraine/1644444))

March 7, 2023 – Gen. Paul Nakasone tells the Senate Armed Services Committee that Russia remains a “very capable adversary” and that “[b]y no means is this done, in terms of the Russia-Ukraine situation.” He adds: “We continue to work very tightly with our other partners within the U.S. government, CISA, FBI, to ensure that our U.S. critical infrastructure is protected, and NATO, in general, to ensure that they’re aware of the tradecraft that the Russians might use.” ([Russia remains a ‘very capable’ cyber adversary, Nakasone says \(c4isrnet.com\)](https://c4isrnet.com/2023/03/07/russia-remains-a-very-capable-cyber-adversary-nakasone-says/))

March 7, 2023 – Representatives of U.S. agencies including USCYBERCOM and the NSA respectively (and anonymously) tell the Voice of America that there is a chance Russian cyber operations will become “bolder” or “increasingly brazen” as the conflict goes on, particularly if the war does not go well for them. The article provides more detail on USG assessments. ([US Bracing for Bolder, More Brazen Russian Cyberattacks \(voanews.com\)](#))

March 7, 2023 – The International Committee of the Red Cross (ICRC) launches a series of “short papers” relating to the applicability of international humanitarian law (IHL) to states’ use of cyber operations in armed conflicts. Special attention is paid to “principles of humanity, necessity, distinction, and proportionality.” The papers can be downloaded from this site: ([IHL and cyber operations during armed conflicts - short papers | ICRC](#))

March 7, 2023 – A cybersecurity firm, Proofpoint, reveals the existence since at least late January 2022 of a Russian email campaign by the group TA499 (aka Vovan and Lexus), which “entices” high-profile individuals critical of the war in Ukraine to expand on their criticisms on phone calls or by video, then posts those comments on YouTube or RUTUBE as a way to cast the individuals in a negative light for Russian audiences. Proofpoint believes the perpetrators are also using video deepfakes in their operations. ([Russian Disinformation Campaign Records High-Profile Individuals on Camera - Infosecurity Magazine \(infosecurity-magazine.com\)](#))

March 8, 2023 – DNI Avril Haines tells the Senate Intelligence Committee that Russia’s heavy losses and poor use of resources in Ukraine have rendered it a less imposing conventional threat but as a result will lead to a greater reliance on “asymmetric” alternatives, including cyberattacks. ([Russia Will Have to Rely on Nukes, Cyberattacks, China: US Intel Chief \(businessinsider.com\)](#))

March 8, 2023 – Ukraine’s SSSCIP publishes “Russia’s Cyber Tactics: Lessons Learned in 2022 – SSSCIP analytical report on the year of Russia’s full-scale cyberwar against Ukraine.” The agency lists the major trends discerned as follows: “Cyberattacks make up an essential component of Russia’s warfare against Ukraine .... Technical vulnerabilities are a key source of hazard alongside phishing .... Hackers are attacking all the institutions they can reach .... Hackers that carry out “quiet” operations are the most dangerous.” ([Russia’s Cyber Tactics: Lessons Learned in 2022 — SSSCIP analytical report on the year of russia’s full-scale cyberwar against Ukraine](#))

March 9, 2023 – Russian strikes against energy facilities across Ukraine cause power outages and Internet disruptions, as detailed by Cloudflare in its Q1 2023 report. Cyberscoop notes that Russia’s operations have shifted toward energy infrastructure and “grown increasingly low tech” as the war has continued. ([Internet disruptions overview for Q1 2023 \(cloudflare.com\)](#); [Russian attacks on Ukrainian infrastructure cause internet outages, cutting off a valuable wartime tool | CyberScoop](#))

March 9, 2023 – The White House releases the Biden administration’s proposed 2024 budget, which includes several mentions of both cybersecurity and support for Ukraine. Among other things, “the Budget requests \$753 million for Ukraine to continue to counter Russian malign influence and to meet emerging needs related to security, energy, cybersecurity, disinformation, macroeconomic stabilization, and civil society resilience.” ([FACT SHEET: President Biden’s Budget Keeps America Safe and Confronts Global Challenges | The White House; budget\\_fy2024.pdf \(whitehouse.gov\)](#))

March 9, 2023 – Anonymous announces the group has resumed its activities against Russia. (The CyberWire, 3-11-2023)

March 10, 2023 – Hackers breach Moscow and Sverdlovsk TV and radio broadcasts with fake warnings that Russia had been hit with a nuclear strike and instructions to take anti-radiation pills and head for the nearest bomb shelter. No-one claimed responsibility for what is reported to be the third such “stunt” in the past few weeks, though Russian authorities blame pro-Ukraine actors. ([Russians told to rush to nuclear bomb shelters after hackers take over state media \(telegraph.co.uk\)](#))

March 10, 2023 – README publishes a take on how the Ukraine war has changed the “global cyberthreat landscape ... but not necessarily in the ways predicted.” Among other points, the article quotes a Mandiant analyst: “In thinking what the future of cyber-enabled conflict looks like, without trying to create too much of an Armageddon-like scenario, realistically, it may look a lot closer to Russia’s usage in Ukraine.” The analyst adds that in the current instance, “It’s wiper malware like CaddyWiper — things that are very, very basic, but that can cause potential disruption, but with limited effects.” ([Russia-Ukraine cyber conflict splits APT groups, raises threat level | by Robert Lemos | Mar, 2023 | README](#) )

March 11, 2023 – The Daily Beast reports on “a major Russian influence operation to destabilize the Moldovan government,” citing U.S. and Moldovan officials. ([Russian Influence Operation Targets Moldova Amid Threats of Coup \(thedailybeast.com\)](#))

March 13, 2023 – The Cipher Brief posts an item based on an interview with Major General Kyrylo Budanov, head of Ukraine’s Main Intelligence Directorate. Aside from predicting that the war will end fairly soon for the simple reason that Russia “cannot drag it out for long,” the 37-year-old Budanov reveals some decidedly low-tech operational practices. These include keeping caged birds in his office to detect “poisonous substances” and receiving most intelligence reporting on paper. “We do this to avoid leaks,” he says. “Everything comes only in paper form. Paper reports can only be obtained, shall we say, if you physically get them, so this way, interception is nearly impossible.” ([Ukraine's Military Intelligence Chief Predicts How War Will End \(thecipherbrief.com\)](#))

March 14, 2023 – Russian warplanes down a U.S. drone over the Black Sea. The Biden administration insists the MQ-9 Reaper was operating in international airspace and the incident was either a “reckless” act or intentional. Before it crashes, operators attempt to wipe clean its electronics. ([Pentagon rejects Russian airspace claims after downing of U.S. drone - The Washington Post](#))

March 14, 2023 – Taiwan has begun producing several drone systems designed for either military strikes or surveillance, in a move the *Japan Times* reports is the result of lessons from the Russian invasion of Ukraine and the latter’s success in developing asymmetric capabilities. ([Taking page from Ukraine, Taiwan shows off new killer drones | The Japan Times](#))

March 14, 2023 – Nataliya Tkachuk, secretary of Ukraine’s National Coordination Center for Cybersecurity, is reported today by *Newsweek* as affirming that Ukraine is drafting legislation to bring volunteer hackers like the IT Army under the purview of the country’s armed forces. “The law on the creation and functioning of cyber forces within the Ministry of Defense of Ukraine should be adopted as soon as possible,” she says. The magazine points to the “legal gray area” of such groups’ status and notes that the IT Army has been criticized for targeting Russian civilian facilities. ([Ukraine Scrambles to Draft Cyber Law, Legalizing Its Volunteer Hacker Army \(newsweek.com\)](#))

March 14, 2023 – Denmark’s Centre for Cyber Security raises the threat level of cyberattacks from medium to high. This change is mainly based on “the high activity from pro-Russian activist hacker groups against NATO countries, including Denmark, as well as on their increased capabilities.” A “high” threat level denotes that authorities deem it likely that Danish organizations will be targets of cyberattacks within two years. (Threat assessment: CFCS raises the threat level of cyberactivism [against Denmark](#) – CFCS)

March 15, 2023 – A new Microsoft report, picked up by the *New York Times* and others, offers “hints” of how the next phases of the “hybrid war” in Ukraine will unfold. For one thing, Microsoft suggests that Moscow’s expected spring offensive may incorporate new cyberattacks. Looking back at the first year of the conflict, the company notes an increase in Russian espionage attacks against at least 17 European nations and a continuation of wiper attacks against Ukraine. Ransomware variants have continued to appear as have “sophisticated influence operations.” The report presents some additional insights, for example: Moscow’s hybrid war “has not gone to plan;” Russian intelligence gathering through cyber has expanded; and “there are no geographical boundaries off limits to attempted Russian attacks.” ([Microsoft Security Compliance and Identity: Russia’s Spring Offensive in Ukraine Could Include Cyberattacks, Microsoft Says - The New York Times \(nytimes.com\)](#))

March 17, 2023 – Microsoft’s Azure Network Security Team releases an analysis of recent activities by Killnet and associated hacker groups targeting healthcare facilities. ([KillNet and affiliate hacktivist groups targeting healthcare with DDoS attacks - Microsoft Security Blog](#))



March 19, 2023 – Ukraine’s SSSCIP warns against streaming unlicensed software: “In many post-Soviet countries, system administrators working for organizations and companies of various forms of ownership still use unlicensed software, including operating systems, shared via torrent trackers. By installing a copy of cracked software from a torrent, they actually give Russian special agencies access to their workstations’ drives. Using cracked operating systems is especially dangerous, as cyber criminals have full administrator access to any device such a system is installed on.” ([Russian hackers spread infected software through torrents \(cip.gov.ua\)](https://cip.gov.ua))

March 19, 2023 – A group of investigative journalists publishes a report based on access to breached files from the Wagner Group. “Dossier Center Investigation: Prigozhin’s Cyber Troops: How the IT Infrastructure of Wagner, Troll Factory and Concorde Works” describes and analyzes the activities of the named entities. ([Dossier Center Investigation: Prigozhin's Cyber Troops \(substack.com\)](https://substack.com)); Risky Biz News, 3-21-2023)

March 21, 2023 – ENISA, the European Union Agency for Cybersecurity, publishes an analysis of the threat to the EU transport sector posed by cyberattacks. The report studies incidents going back to early 2021 and looks for trends in addition to listing key actors and threats. ([ENISA Transport Threat Landscape — ENISA \(europa.eu\)](https://europa.eu))

March 21, 2023 – An opinion piece in The Cipher Brief presents U.S. information-sharing with allies and the public about Russia’s plans to invade Ukraine as evidence of the value of, and need for, “maximizing the analytic power of open source and public data.” Chris Rasmussen, a veteran of 20 years in the Intelligence Community, argues: “OSINT and the sub-discipline social media intelligence (SOCMINT) are often bound within classified frameworks where flexibility is limited.” What is required is “a new independent OSINT agency outside the IC” which would be “built from the ground up, not to protect secrets, but to create quality and shareable OSINT at scale with sufficient full-time OSINT practitioners in large numbers enabled by remote and hybrid telework, limited security clearances, and the rapid growth of the OSINT knowledge base at the unclassified level for broad dissemination, not sucked to the highside as a supplement to classified operations.” ([Avoiding the Secrecy Trap in Open Source Intelligence \(thecipherbrief.com\)](https://thecipherbrief.com))

March 22, 2023 – Mandiant releases a report on a rising trend in which hacktivist groups claim, either falsely or with exaggeration, to target “operational technology” (OT) systems with harmful attacks. Mandiant concludes that ideological motives are behind many of these incidents, most of which in the past year were carried out by supporters of Ukraine in the current conflict. The company also observed some attacks that favored Russia and others that targeted organizations in the Middle East. Mandiant has determined with moderate confidence that the actors involved have typically overstated the results and implications of their strikes. ([We \(Did!\) Start the Fire: Hacktivists Increasingly Claim Targeting of OT Systems | Mandiant](https://www.mandiant.com))

March 22, 2023 – The New York Times reports on increasing Kremlin efforts to crack down on social media postings it deems to be critical of the war in Ukraine. The focus of the story is a 20-year-old university student named Olesya Krivtsova. ([Russian Faced Prison Time for Instagram Post About War in Ukraine - The New York Times \(nytimes.com\)](https://www.nytimes.com/2023/03/22/world/europe/ukraine-russia-social-media.html))

March 22, 2023 – Bloomberg posts an item exploring the propaganda group Ghostwriter, which has a history of spreading false information and forged documents designed to alarm supporters of Ukraine. The article quotes Jānis Sārts, director of NATO's Strategic Communications Center of Excellence, as saying he has “no doubt” that the group is Russian, “even if some of it went through Belarus.” ([Ukrainian Refugees Targeted by 'Ghostwriter' Propaganda Group With Fake Emails - Bloomberg](https://www.bloomberg.com/news/articles/2023-03-22/ukrainian-refugees-targeted-by-ghostwriter-propaganda-group-with-fake-emails))

March 22, 2023 – The Atlantic Council publishes an articles in its “5x5” monthly Cyber Statecraft Initiative series. Five experts (Nika Aleksejeva, Silas Cutler, Roman Osadchuk, Emma Schroeder, and Gavin Wilde) answer five questions about the “conflict in Ukraine’s information environment.” ([The 5x5—Conflict in Ukraine's information environment - Atlantic Council](https://www.atlanticcouncil.org/5x5/2023/03/22/the-5x5-conflict-in-ukraine-information-environment/))

March 22, 2023 – Foreign Policy hosts a forum to discuss nuclear cybersecurity against the background of Russia’s seizure of the Zaporizhzhia nuclear plant. (Video available at: [FP Virtual Dialogue: Enhancing Cyber Nuclear Security – Foreign Policy](https://www.foreignpolicy.com/events/2023/03/22/fp-virtual-dialogue-enhancing-cyber-nuclear-security/))

March 24, 2023 – Ukraine’s government approves a resolution requiring information security audits for certain categories of critical infrastructure facilities every two or three years. Aggregated results will go to the National Security and Defense Council. ([The Cabinet has approved a Resolution regulating introduction of independent audits of information security systems at critical infrastructure facilities \(cip.gov.ua\)](https://www.cip.gov.ua/en/news/2023/03/24/the-cabinet-has-approved-a-resolution-regulating-introduction-of-independent-audits-of-information-security-systems-at-critical-infrastructure-facilities))

March 25, 2023 – BleepingComputer reports that Rostekh, which monitors information flows in Russia, has apparently bought a platform enabling it to figure out the identities of users of Telegram. Reportedly named “Hunter” (Охотник), it is supposed to be able to use more than 700 data points from internet platforms of various kinds to make connections to users. Rostekh is expected to make the technology available to the FSB this year. Telegram provides a response to the news outlet explaining ways that users can de-anonymize themselves inadvertently. ([Russia’s Rostec allegedly can de-anonymize Telegram users \(bleepingcomputer.com\)](https://www.bleepingcomputer.com/news/ukraine/russia-rostec-allegedly-can-de-anonymize-telegram-users/))

March 27, 2023 – Hacker group NoName claims it conducted a successful DDoS attack on the website of France’s National Assembly earlier this morning. It is one of a series of such attacks in the past week on European governments and private companies, each of which have taken a pro-Ukraine stance. ([Russian Hackers Target French National Assembly Website \(privacyaffairs.com\)](https://www.privacyaffairs.com/en/2023/03/27/russian-hackers-target-french-national-assembly-website/))

March 27, 2023 – Ukraine’s SSSCIP tweets about the evolution of Russian cyberattacks. "While central government remains a major target for russian #hackers, we also record a significant number of attacks on local-level authorities (second largest number of attacks). Security and defense sector used to be ranked second a year ago." The SSSCIP adds: "Cert-UA is recording a certain drop in the number of #cyberattacks on the security and defense sector and a growing amount of incidents in the public sector, as well as attacks on software developers, Internet service providers, and commercial companies." (The CyberWire, 3-28-2023)

March 27, 2023 – Radware posts a breakdown of key pro-Russian hacker groups that have sprouted in response to Ukraine and the West’s actions against Russia following its invasion of Ukraine. ([Pro-Russian Hacktivists: A Reaction to a Western Response to a Russian Aggression | Radware Blog](#))

March 27, 2023 – According to an account today, Ukrainian hacktivists “Cyber Resistance” have turned over to InformNapalm a dump of emails and other private correspondence of a Russian colonel, Sergei Atroshchenko, said to be the commander of Russia’s 960<sup>th</sup> Assault Aviation Regiment, a unit alleged to have bombed civilian facilities in Mariupol early in the war. The materials have been handed to the International Criminal Court. The hackers went further by persuading the wives of Atroshchenko’s squadron to do a photo shoot of themselves in their husbands’ uniform jackets. ([The hacking of a Russian war criminal, commander of military unit 75387, 960th assault aviation regiment \(informnapalm.org\)](#); [Ukrainian group reveal Russian pilots who bombed Mariupol theatre \(telegraph.co.uk\)](#))

March 28, 2023 – The International Institute for Strategic Studies (IISS) publishes a study of Ukraine’s success defending against Russian cyberattacks in the current war. Author Dan Black of Mandiant concludes that early action and practicing “sound defensive fundamentals” have both been crucial to Kyiv’s efforts. Questions raised by the experience include how “durable” the “Ukrainian model” is, what else can be done on Kyiv’s behalf, and exactly how relevant is Ukraine’s experience likely to be for future conflicts. ([russias-war-in-ukraine-examining-the-success-of-ukrainian-cyber-defences.pdf \(iiss.org\)](#))

March 29, 2023 – The acting deputy head of the Security Service of Ukraine’s (SSU) Cybersecurity Department, Ivan Kalabashkin, blames Moscow for up to 1,200 critical cyber incidents during the first quarter of 2023. ([Russia Ramping Up Cyberattacks Against Ukraine \(voanews.com\)](#))

March 29, 2023 – ThreatMon publishes “In-Depth Analysis on the Roles of Threat Actors and Attacks in the Ukraine-Russia War: Anonymous Russia.” It is the third in a series probing threat actors in the current conflict. It details a series of Anonymous Russia attacks starting on July 10, 2022. ([Anonymous Russia: Analysis of Threat Actors in Ukraine-Russia War \(threatmon.io\)](#))

March 29, 2023 – The Royal United Services Institute for Defence and Security Studies (RUSI) releases a report on “Preliminary Lessons from Russia’s Unconventional Operations during the Russo-Ukrainian War, February 2022–February 2023.” It assesses Russia’s agent network, its strengths and weaknesses, plans, use of human intelligence, and other facets of operations. ([Preliminary Lessons from Russia's Unconventional Operations During the Russo-Ukrainian War, February 2022-February 2023 \(rusi.org\)](#))

March 30, 2023 – Proofpoint’s threat insight team reports on observations of TA473 (Winter Vivern, UAC-0114), described as a “newly minted advanced persistent threat (APT) actor” whose goal “is assessed to be gaining access to the emails of military, government, and diplomatic organizations across Europe involved in the Russia Ukrainian War.” ([Exploitation is a Dish Best Served Cold: Winter Vivern Uses Known Zimbra Vulnerability to Target Webmail Portals of NATO-Aligned Governments in Europe | Proofpoint US](#))

March 30, 2023 – A trove of some 5,000 stolen records from a Russian contractor closely tied to the GRU forms the basis of a major piece in the *Washington Post* and other news outlets. While indicating that the connections between the Russian government and private cyber firms are tight, none of the articles point to specific attacks by Russia or provide access to the original records. (See also April 18, 2023, entry) ([The Vulkan Files: Secret trove offers rare look into Russian cyberwar ambitions - The Washington Post](#))

Late March 2023 – Russian financial cybercrime group FIN7 exploits software vulnerabilities to steal stored credentials from servers running Veeam Backup & Replication. In April, WithSecure Intelligence, a cybersecurity firm, discovers and reveals the two main attacks. ([FIN7 tradecraft seen in attacks against Veeam backup servers – WithSecure](#))

April 3, 2023 – Retired Adm. James Stavridis accuses the West of “digital appeasement” in the face of prolonged Russian aggressive behavior, in both the kinetic and cyber spheres. Writing in the *Washington Post*, he lists a string of cyberattacks against Ukraine since 2015 that he says led in recent days to “the biggest denial-of-service attack in the country’s history,” followed by a major military thrust. He charges that “far too often the West has failed to respect cyberwarfare’s role as a strategic instrument of power projection,” adding that “[c]yberattacks are at the heart of Putin’s so-called hybrid warfare, central to the current Kremlin playbook.” “Western allies have allowed Russia to act virtually unchallenged ... evoking legitimate comparisons of European appeasement of the Nazis in the lead-up to World War II.” He goes on to offer explanations for “this modern-day form of digital appeasement.” ([The West’s Cyber Appeasement Helped Give Putin a Green Light - The Washington Post](#))

April 3, 2023 – CyberResistance, a hacktivist group aligned with Ukraine, alleges that they broke into the AliExpress account of a Russian military blogger named Mykhayl



Luchin and bought \$25,000 worth of dildos using a linked payment card. ([Telegram: Contact @cyberResistanceUA](#); [\(2\) Risky Biz News: UK government confirms NCF offensive cyber operations \(substack.com\)](#))

April 3, 2023 – ThreatMon publishes “In-Depth Analysis on the Roles of Threat Actors and Attacks in the Ukraine-Russia War: IT Army of Ukraine.” ([IT Army of Ukraine: Analysis of Threat Actors In The Ukraine-Russia War \(threatmon.io\)](#))

April 4, 2023 – The Lawfare Podcast broadcasts the annual Breyer Lecture on International Law at the Brookings Institution featuring Oona Hathaway of Yale Law School, who discusses the surprisingly strong response to the Ukraine war from legal sector. ([The Lawfare Podcast: Russia’s Aggression Against Ukraine and the International Legal Order - Lawfare \(lawfareblog.com\)](#))

April 5, 2023 – European cybersecurity firm Thales publishes “2022-2023: A Year of Cyber Conflict in Ukraine.” It notes a significant shift in Russian tactics starting in the third quarter of 2022 toward a focus on targets outside Ukraine, particularly the Baltics, Scandinavia, and Poland. ([From Ukraine to the whole of Europe:cyber conflict reaches a turning point | Thales Group](#))

April 5, 2023 – The Health Sector Cybersecurity Coordination Center (HC3) of the U.S. Department of Health and Human Services publishes an Analyst Note on the pro-Russia hacktivist group KillNet and its operations targeting the public health sector between December 2022 and March 2023. ([202304051200 KillNet Analyst Note TLPWHITE \(hhs.gov\)](#))

April 6, 2023 – The *New York Times* breaks a story on a “trove” of leaked Pentagon documents on the war in Ukraine and many other topics that have been posted on the chat platform Discord. Subsequent media reports label it “one of the worst national security leaks in U.S. history.” Meanwhile, Ukrainian leaders say they are unconcerned about the impact on their operations because they routinely withhold the most sensitive information from their American allies precisely in order to prevent unwanted disclosures. ([Ukraine War Plans Leak Prompts Pentagon Investigation - The New York Times \(nytimes.com\)](#); [How classified US documents quickly spread from gamer chat rooms to the rest of the internet | DC News Now](#); [US, Ukraine say many war secrets safe from intel leaks \(c4isrnet.com\)](#))

April 6, 2023 – Recorded Future issues a report on the hacktivist threat group Joker DPR, which has mainly used Telegram to spread pro-Russian and anti-Ukrainian propaganda. The group is said to rely on Ukrainians sympathetic to the Kremlin. Its biggest claimed success has been a reported breach of the Delta battlefield management system. ([Joker DPR and the Information War \(recordedfuture.com\)](#))

April 7, 2023 – Ukrainian law enforcement authorities have uncovered a \$40 million crypto pyramid scheme operating out of an office in Kyiv but originally based in Russia

prior to 2017, according to a media report today. ([\\$40 Million Crypto Pyramid Scheme Busted in Ukraine \(beincrypto.com\)](#))

April 10, 2023 – InformNapalm posts personal information about Lt. Col. Sergey Alexandrovich Morgachev, described as part of the GRU, leader of APT28, and wanted by the FBI. (Morgachev is wanted for his role in hacking the Hillary Clinton and other campaigns in 2016.) InformNapalm obtained the data from the Ukrainian hacktivist group Cyber Resistance. ([Hacked: Russian GRU officer wanted by the FBI, leader of the hacker group APT 28 \(informnapalm.org\)](#); [Fake ChatGPT preys on Facebook users - The Washington Post](#))

April 10-11, 2023 – James Rubin, a special State Department envoy and coordinator of the department's Global Engagement Center, visits the Balkans to strategize with local governments on how to contend with Russian and Chinese disinformation, including such measures as identifying Facebook pages that are being used to spread propaganda. ([U.S. Steps Up Effort to Fight Against Russian Disinformation - WSJ](#))

April 11, 2023 – NATO replies to a request from CyberWire for comment on recent reports that KillNet launched DDoS attacks against the alliance. The comment notes: "We are currently experiencing Denial of Service attempts against a number of NATO websites, and our experts are responding. NATO's classified networks are not affected and there is no impact on NATO operations." CyberWire notes that a principal target was the NATO School Oberammergau, which is not an operational command. (The CyberWire, 4-11-2023)

April 11, 2023 – Rob Joyce, director of cybersecurity at the National Security Agency, tells attendees at a CSIS event that Russian-backed hackers continue to look for creative ways to conduct surveillance in Ukraine, including tapping into local closed circuit security cameras in coffee shops, "to watch convoys and trains delivering aid." ([Russian hackers 'target security cameras inside Ukraine coffee shops' | Ukraine | The Guardian](#))  
Joyce adds that Moscow is still a serious cyber threat: "In cyber, I think people have underestimated really how much game they [Russia] brought, whether it be the Viasat hack to nine or 10 different families of brand-new, unique wiper viruses that have been thrown in that ecosystem." ([US Warns Russia Getting Creative in Cyberspace \(voanews.com\)](#))

April 11, 2023 – A DDoS attack temporarily blocks Canadian Prime Minister Justin Trudeau's government website on the same day he is set to meet with his Ukrainian counterpart, Denys Shmyhal. Trudeau tells a press conference that "Russia being able to bring down an official government of Canada web page for a few hours is in no way going to dissuade us from our unshakable support of Ukraine." ([DDoS attacks block PM Trudeau's web site | IT World Canada News](#))

April 12, 2023 – Nikkei Asia reports that hundreds of millions of dollars' worth of American-made semiconductors continue to be shipped to Russia in spite of

sanctions. Nikkei's source is Russian customs data provided by an Indian research company and covers the period February 24 – December 31, 2022. (See December 31, 2022, entry) ([Special report: How U.S.-made chips are flowing into Russia - Nikkei Asia](#))

April 13, 2023 – The Polish prime minister's cybersecurity department releases the following: "The Military Counterintelligence Service and the CERT Polska team (CERT.PL) [has] observed a widespread espionage campaign linked to Russian intelligence services, aimed at collecting information from foreign ministries and diplomatic entities. Most of the identified targets of the campaign are located in NATO member states, the European Union and, to a lesser extent, in Africa."

The announcement notes that there is much apparent overlap with activity by the entity known variously as Cozy Bear, NOBELIUM, and APT29, although the use of certain software represents a new element. ([Espionage campaign linked to Russian intelligence services - Baza wiedzy - Portal Gov.pl \(www.gov.pl\)](#))

April 13, 2023 – Ukraine's National Agency on Corruption Prevention (NACP) declares that Chinese smartphone maker Xiaomi has "not only continued its work in the Russian Federation after the full-scale invasion [of Ukraine], but is still the leader in smartphone sales in the terrorist state." Xiaomi responds that it is not supporting the war and is following all laws and regulations. ([Ukraine puts Chinese smartphone giant Xiaomi, CEO Lei Jun on war sponsor list over business in Russia | South China Morning Post \(scmp.com\)](#))

April 14, 2023 – The German automotive and arms manufacturer Rheinmetall is hit with a ransomware attack later confirmed to be launched by the Black Basta group. The company is said to be a critical part of the war in Ukraine and had been reported to be negotiating over the building of a new tank factory in the country. ([German arms company Rheinmetall confirms Black Basta ransomware group behind cyberattack \(therecord.media\)](#))

April 15, 2023 – Killmilk, leader of Killnet, reveals the real identity of the head of Anonymous Russia, another group conducting DDoS attacks in Ukraine. According to Killmilk's Telegram channel, the head of Anonymous Russia was an 18-year-old Belarusian, who was subsequently arrested due to the presence of a Belarusian government agent who had infiltrated the group. According to Flashpoint, a business risk intelligence company, this situation points to larger clashes between different pro-Russia hacktivist groups, as Killnet attempts to bring in other groups under its own leadership. ([Killnet Ostracizes Leader of Anonymous Russia, Adding New Chapter to Pro-Kremlin Hacktivist Drama](#) – Flashpoint)

April 18, 2023 – Dragos publishes an analysis of documents leaked from a Moscow-based contractor, NTC Vulkan, that purport to describe contracts between it and the Russian Ministry of Defense. The report studies the question of what kind of threat to critical infrastructure is posed by the cyber program covered by the contracts. The main cyber program in question is dubbed Amesit-B, which Dragos describes as

an “offensive computer network operations platform that includes signals intelligence (SIGINT), electronic warfare (EW), and malign influence capabilities.” ([Dragos IntelBrief Russian-Programs-Threatening-Critical Infrastructure.pdf](#))

April 18, 2023 – The U.K.’s NCSC along with the NSA, CISA, and FBI publish a joint advisory “to provide details of tactics, techniques and procedures (TTPs) associated with APT28’s exploitation of Cisco routers in 2021.” The agencies assess that APT28 is “almost certainly” the GRU’s 85th special Service Centre (GTsSS) Military Intelligence Unit 26165. APT28 is also known as Fancy Bear, STRONTIUM, Pawn Storm, the Sednit Gang and Sofacy. In 2021, about 250 Ukrainian entities were among its targets. ([APT28 exploits known vulnerability to carry out... - NCSC.GOV.UK](#))

April 18, 2023 – A report on the state of Ukraine’s digital operations and future cyber goals, written by two analysts from the Carnegie Endowment for International Peace who recently visited the country, is published Cyberscoop. ([How cyber support to Ukraine can build its democratic future | CyberScoop](#))

April 18, 2023 – The Carnegie Endowment for International Peace releases a paper, “Integrating Cyber Into Warfighting: Some Early Takeaways From the Ukraine Conflict.” Written by former Israeli nuclear official Ariel (Eli) Levite, the 40-page report notes: “Some of the propositions we advance are novel; others reaffirm or refine tentative assertions made before the war. Taken together they suggest a more subdued view of the utility and impact of cyber warfare than was generally found in prewar speculations. More importantly, the Ukraine war reveals that nations diverge significantly in the role and aims they assign to offensive cyber operations as well as the institutional setup and operational modalities they use for conducting them. Most glaringly, the U.S. perspective and approach (emulated in whole or in part by several other Western nations) differs deeply from that of Russia, which makes it reasonable to expect similar divergence across similar regimes.” ([Levite Ukraine Cyber War.pdf \(carnegieendowment.org\)](#))

April 18, 2023 – Avast Threat Labs releases a report on Project DDosia, an initiative from pro-Russia hacktivist group NoName057(16) that targets Ukrainian and NATO organizations. The report determines that the group is still conducting DDoS attacks, paying people with cryptocurrency to install their tool. In addition to the Python version seen last year, the group has recently released a Go variant of bots as well. ([DDosia Project: How NoName057\(16\) is trying to improve the efficiency of DDoS attacks – Avast](#))

April 18, 2023 – The European Commission publishes the first draft of the EU Cyber Solidarity Act, which includes several initiatives to improve cybersecurity across the EU and standardize incident response plans, including creating a “cyber shield” tasked with collecting “high quality” intel on cyberthreats. ([Proposed Regulation on the Cyber Solidarity Act – European Commission](#))



April 19, 2023 – Poland's Ministry of National Defense claims that Ghostwriter, a Belarusian hacking group, has launched their third disinformation campaign against Poland since the beginning of 2023. The campaign consisted of messages trying to scare Polish citizens, saying they were being drafted and sent to fight for the Ukrainian army. The Polish government attributes the campaign to Ghostwriter unusually quickly, due to the recurrent nature of the disinformation attack. ([Disinformation Operation Against RP Underway](#) – Ministry of National Defense)

April 19, 2023 – The U.K.'s National Cyber Security Centre (NCSC) issues an alert concerning threats to critical infrastructure from state-aligned groups, particularly ones that support Russia in its war in Ukraine. Dr. Marsha Quallo-Wright, NCSC deputy director for critical national infrastructure, notes that some groups intend to “cause damage” to CNI organizations. That implies doing more than routine DDoS attacks. ([NCSC warns of emerging threat to critical national... - NCSC.GOV.UK](#))

April 19, 2023 – The U.K.'s Ministry of Defence releases an intelligence update noting a unique element of Russia's disinformation campaigns: “narrative laundering,” where information is first promoted through proxies or smaller, unverified sources. Then, the disinformation is picked up by mainstream media, despite the obscurity of the original source, “making it easier for the Russian state to distance itself from the message.” ([Intelligence Update](#) - Ministry of Defence)

April 19, 2023 – ABC (Australia) publishes an article that includes excerpts of an interview with “Kerasid,” a hacker who claims to be 0\_neday, one of the leaders of Russia-affiliated REvil. (ABC could not confirm that.) The article describes how ransomware groups like Conti are set up, with dozens of employees, HR departments, and incentive structures including employee of the month; it also offers some insights into pro-Russian hacker attitudes, notably Kerasid's highly derogatory views of Australians (“the most stupidest humans alive”) and Americans and his brutally unsympathetic take on the impact of ransomware attacks on health care industry firms such as Medibank, which Kerasid claims to have participated in. ([Chatting with a hacker about cybercrime gangs, Medibank and supporting Russia's attacks on Ukraine - ABC News](#))

April 19, 2023 – Google's Threat Analysis Group (TAG) releases a report detailing how Russian hackers are adapting their tactics, including continuing Russian government-backed phishing campaigns and targeting Europe's energy sector. The report identifies Russian military intelligence hacker group known as Sandworm as the most versatile threat, targeting areas of interest for Russian intelligence. ([Ukraine remains Russia's biggest cyber focus in 2023](#) – TAG)

April 19, 2023 – Pro-Russia hacker group Killnet attacks Eurocontrol, Europe's air traffic control authority, in a “marathon” lasting 100 hours, according to Eurocontrol. While flights have been unaffected, the attack is causing web availability interruptions. ([European air traffic control says attack by ‘pro-Russian hackers’ not affecting flights – CNN](#))

April 20, 2023 – Killnet leaks the data of nearly 5,000 individuals with ties to NATO, along with various documents detailing KillNet’s version of NATO history. ([Pro-Russian KillNet targets thousands with ties to NATO](#) – CyberNews)

April 21, 2023 – The European Cyber Conflict Research Initiative issues a report on a conference that examined methods of Russian cyberattacks. The report’s takeaways include that “distinguishing between cyber criminal and political activist groups is becoming increasingly difficult,” as well as the fact that “Western observers may overestimate coordination between Russian-aligned criminals and the government.” ([The Cyber Dimensions of the Russia-Ukraine War](#) – ECCRI)

April 21, 2023 – Radware releases a report on the current state of hacktivism, noting that groups acting as cyber auxiliaries to the Russian government have launched a growing number of DDoS attacks. The report states that “Killnet, the group most prominently covered in the media and suspected of most hacktivist DDoS activity, did not make the top 15 of hacktivists claiming DDoS attacks in the last two months. NoName057(16), who does not want to be associated with Killnet, is by far the most active DDoS hacktivist amongst the politically driven, pro-Russian hacktivists.” ([Hacktivism Unveiled, April 2023 Insights Into the Footprints of Hacktivists](#) – Radware)

April 24, 2023 – Palantir announces an agreement with the Prosecutor General’s Office of Ukraine to process all key data relating to more than 78,000 alleged war crimes. ([Palantir to Support Ukrainian Prosecutor-General’s Investigation into War Crimes](#) – Business Wire)

April 24, 2023 – Ukraine strikes the main Crimean naval base in Sevastopol with a drone, according to Russian authorities. AP News notes that this attack is the latest of several Ukrainian drone strikes, as Ukraine prepares for a counteroffensive. ([Drones attack Sevastopol, crashed drone found near Moscow](#) – AP News)

April 24-27, 2023 – The RSA security conference in San Francisco takes place, which, according to *Politico*, serves as a setting for top Ukrainian cyber officials to garner more support and resources from the U.S. While no formal deals are agreed upon at the conference, Ukrainian officials received commitments from both private and public U.S. partners. Illia Vitiuk, head of the Department of Cyber and Information Security at the Security Service of Ukraine, mentions that he spent the conference in constant meetings with U.S. associates. ([Ukraine uses annual hacker confab to gather support for cyber aid from the U.S.](#) - Politico)

April 25, 2023 – An FBI official notes that the Bureau has been helping Ukraine to gather and process vast amounts of information related to Russian cyberattacks on civilian infrastructure. According to Ukrainian officials, they hope to obtain and sort out data from U.S. organizations with the help of the FBI, such as fingerprints or cell phone locations. While cyberattacks on civilian infrastructure have never been prosecuted as war crimes before, with this organized data Ukraine hopes to bring

successful charges for the first time against Russia. ([FBI aiding Ukraine in collection of digital and physical war crime evidence](#) – CyberScoop)

April 26, 2023 – The Ukraine government launches the BRAVE1 initiative which is designed to advance innovation with drones and other critical technologies. Ukraine's defense minister declares that this initiative is the next step towards gaining more independent military capabilities. ([Ukraine's government launches initiative to streamline development of drones, other technologies used in war](#) – FOX)

April 26, 2023 – NSA's director of cybersecurity, Rob Joyce, notes that Russia has been focusing on disrupting Ukraine's logistics supply chain with ransomware, rather than solely focusing on critical infrastructure, as was previously anticipated. He also declares that European or U.S. online militias – non-government affiliated "hactivist" groups – working to support Ukraine only "add to the noise," impacting the U.S.' ability to set cyber norms and giving Russia leeway to make disinformation claims against Western countries. ([NSA cyber director warns of ransomware attacks on Ukraine, Western supply chains](#) – The Record)

April 26, 2023 – The Cyber Police of Ukraine arrest a Ukrainian citizen for allegedly selling the personal data of over 300 million people to Russian citizens. The Ukrainian police note he administrated closed groups on Telegram, where he would sell Ukrainian and EU citizens' data, such as passport and bank account information, to Russian citizens. ([The cyber police exposed an attacker in the sale of databases with personal data of citizens of Ukraine and the EU](#) – Cyber Police UA)

April 27, 2023 – KillNet's leader posts on Telegram that the group will now be known as a "private military hacking company." According to CyberNews, "The term 'private military company' or PMC has become a sign of toughness in the context of the war in Ukraine since Yevgeny Prigozhin started publicly promoting PMC Wagner." This shift in name can be seen as an attempt for the group to be taken more seriously, according to Nataliia Zdruk, a threat intelligence analyst at cybersecurity firm Binary Defense. ([Killnet: we are now a private military corporation](#) – CyberNews)

April 28, 2023 – According to Ukraine's Computer Emergency Response Team (CERT), GRU actor APT28 is responsible for sending phishing emails to various Ukrainian government agencies throughout April. The hackers are impersonating Ukrainian government system administrators, and the emails supposedly contain instructions on how to update Windows to defend against cyberattacks. Instead, the instructions lead users to also install a PowerShell script in the background that uses information-harvesting malware. ([APT28 cyberattack: distribution of emails with "instructions" on "updating the operating system"](#) – CERT-UA)

May 2023 – Georgetown's Center for Security and Emerging Technology (CSET) holds a workshop with experts and former government officials resulting in a report on the critical role U.S. tech companies have played in the war. The report details how U.S. tech companies can better support U.S. strategic interests and help to defend

Ukraine, mainly including increased collaboration between the public and private sectors. ([U.S. Tech Companies and Their Contributions in Ukraine](#) – CSET)

May 1, 2023 – Chainalysis discovers a leak by a hacker who released 986 Bitcoin addresses that were allegedly used by Russian intelligence services. Three of the addresses were previously used by Russian intelligence in past operations, including SolarWinds. (Hacker exposes 986 Bitcoin addresses operated [by Russian intelligence agencies](#) – RiskyBiz News)

May 5, 2023 – CERT-UA cautions that Russian criminal group UAC-0006 is spreading SmokeLoader malware in a phishing campaign, compromising the target's financial activities and passwords. ([Reverting UAC-0006: Mass distribution of SmokeLoader using "accounts" theme](#) – CERT-UA)

May 9, 2023 – Several U.S. government agencies release a joint cybersecurity advisory detailing the FBI "Operation MEDUSA" that disrupted nearly 20-year-old malware used by Turla, one of Russia's cyberespionage units in their Federal Security Service (FSB). The malware called "Snake," which officials noted was the FSB's "most sophisticated cyber espionage tool," was used to access sensitive documents and information from hundreds of computer systems in at least 50 countries, according to the U.S. Department of Justice. Notably, the formal connection of Turla APT to the FSB is the first time a foreign government has officially linked the two. ([Hunting Russian Intelligence "Snake" Malware](#) – Joint Cybersecurity Advisory)

May 11, 2023 – The IRS helps out Ukrainian authorities trying to stop Russians from using cryptocurrency to avoid sanctions by holding an advanced blockchain analysis training for Ukrainian law enforcement. ([IRS Trains Ukraine Law Enforcement to Track and Trace Russia's Cryptocurrency Moves](#) – Decrypt)

May 12, 2023 – On Telegram, Killmilk, spokesperson for Killnet, expresses uncertainty that the group will be able to fully make the switch to a private military hacking company. CyberWire reports that, according to Killmilk, "while attempting to acquire more servers for their botnet, he had drawn the attention of the FBI and, as a result, the organization's botnet was seized." It is currently unclear if this was related to the FBI's takedown of Snake malware (see May 9, 2023 entry). Lastly, Killnet also announced the release of their own OSINT tool, although the tool is limited due to its scope of only searching Russian-owned social media and public databases, conflicting with Killnet's pledge not to operate against or inside of Russia. (The Cyberwire 5.12.23: Babuk resurfaces. Alert on PaperCut vulnerabilities. Too many bad bots. KillNet's [PMHC regrets](#). - CyberWire)

May 14, 2023 – According to Bloomberg, Anonymous Sudan is not an Islamist Sudanese hacktivist group, as they present themselves, but actually an operation of Russian intelligence services targeting Sweden. According to Katarzyna Zysk, a professor of international relations at the Norwegian Institute for Defence Studies in Oslo, one goal of these attacks is to delay Sweden's NATO membership through DDoS attacks



as well as influence operations targeting Sweden's Muslim minority and at Turkish public opinion. ([Posing as Islamists, Russian Hackers Take Aim at Sweden](#) – Bloomberg)

May 17, 2023 – With a unanimous vote, Ukraine officially becomes a “contributing participant” of NATO's Cooperative Cyber Defence Centre of Excellence (CCDCOE). While Ukraine and CCDCOE have been cooperating since shortly after Russia's invasion, Ukraine's status is now formal. ([Ukraine to be accepted as a Contributing Participant to NATO CCDCOE](#) – CCDCOE)

May 18, 2023 – Polish news websites are hit with DDoS attacks from Russian hacking groups, according to Poland's digitalisation minister. ([Polish news websites hit by DDoS attacks](#) – Reuters)

May 21, 2023 – In an interview with The Record, the head of Ukraine's State Service of Special Communications and Information Protection (SSSCIP), Yuriy Shchychol, notes the shifts in Russian cyber operations over the course of the war. According to Shchychol, Russia is focusing more on the private sector, in addition to shifting away from destructive malware to focusing on information collection. ([Ukraine's cyber chief on the ever-changing digital war with Russia](#) – The Record)

May 25, 2023 – Mandiant publicizes the discovery of a new Russian-linked malware called CosmicEnergy, which remotely tampers with power lines and circuit breakers, posing a threat to electrical grids. (COSMICENERGY: New OT Malware Possibly Related To [Russian Emergency Response Exercises](#) – Mandiant)