Research Paper

Russia and Eurasia Programme

December 2023

Russian cyber and information warfare in practice

Lessons observed from the war on Ukraine

Keir Giles

CHATHAM HOUSE

Chatham House, the Royal Institute of International Affairs, is a world-leading policy institute based in London. Our mission is to help governments and societies build a sustainably secure, prosperous and just world.

Contents

Summary

- Russia's use of cyber and information warfare against Ukraine has confirmed some previous assessments of Russian doctrine and capabilities and invalidated others. In both cases, observation of operations in the war to date provides valuable insights for other states and coalitions seeking to defend themselves effectively against Russia in the future.
- Russia's operations in Ukraine have provided a clear practical demonstration of the holistic and integrated nature of Russia's approach to using information for effect in wartime conditions. This implies that potential future victims of Russian aggression should recognize the crucial interdependencies this approach exploits – not only between cyber and information activities but also between these and the physical environment and cognitive domain – and adjust defensive strategies accordingly.
- In particular, information and assets not normally thought to be targets for combat operations must be protected. Private personal information captured before and during military operations has been used by Russia with lethal consequences for its subjects.
- Ukraine's successful resistance to Russian cyber campaigns has been substantially enabled by support from international partners but also, critically, from private industry. The involvement of private industry in hostilities raises issues of accountability and legal status, as well as the question of financial and other support for the organizations offering their services. These issues should be addressed as a matter of urgency so that policies are in place before they are next required.
- The participation of private citizens in information activities as part of the defence of Ukraine potentially undermines the notional protection they are afforded as civilians rather than combatants. While there is no expectation that Russia will observe international humanitarian law, this has the potential to complicate eventual prosecutions for breaches of it.
- This research paper offers policy recommendations for enhancing the resilience of Western states to cyber and information operations by Russia. These recommendations, by their nature, will also be relevant for protection against any other state or non-state threat actor seeking to exploit similar vulnerabilities.

01 Introduction

Russia's full-scale war on Ukraine since February 2022 has led to many previous assessments of Russian military power being revised. This research paper examines Russia's campaigns and Ukraine's responses in the cyber and information aspects of the conflict.

This research paper surveys cyber and information activities observed in the context of Russia's war on Ukraine in the period after February 2022. Its aim is to understand the nature of those activities, the principles informing them, and to determine whether lessons can be drawn that will assist in preparing for the information element of future confrontations with Russia, up to and including major conflict involving the United States or other NATO nations.

With that in mind, this paper refers to a number of specific instances of cyber and information operations against Ukraine or its backers, but the objective is not to dissect these operations in detail. This is not a technical report on cyber activities; instead, the aim is to observe patterns of behaviour and effects, and determine whether they provide useful pointers for the future.

Scope and definitions

This paper considers both cyber activities – those affecting technical systems and networks – and information operations – those seeking to bring about a cognitive effect on humans. Despite recent evolution in doctrinal approaches in a number of Western nations, these two areas of warfighting have not always sat comfortably

together in defence and security thinking in much of the Euro-Atlantic area.[1] Yet Russian concepts treat these two lines of effort – 'information-technical' and 'information-psychological' activities – as implicitly integrated.[2] And since this is a war waged by Russia, any framing of operations other than the Russian one risks being misleading.

It follows that it is important to ground our understanding of Russian actions in Russia's own concept of 'information confrontation'.[3] A current Russian definition for information confrontation describes it as 'a form of conflict between parties… each of which attempts to cause the other defeat or damage by means of informational impact… [it has become] a form of combat in which information is both the tool, the environment, and the target'.[4] Crucially, the 'environment' includes not only computers, other endpoints, and digital and cyber-physical networks. Its definition is much broader – encompassing, for example, public opinion in a target state and the thought processes of individual decision-makers. The reason for adopting this framing will become clear throughout this paper, given the multiple instances it documents of overlapping and interdependent effects between these domains – for example, between Russia's attacks on Ukrainian technical capabilities or infrastructure and its use of disinformation or other tactics to attempt to manipulate opinion. An important factor here is the dependence of Russian cyber and information warfare on both the physical environment and human factors for its effectiveness. The paper thus includes a chapter on information effects designed to influence Ukrainian or Western policy primarily through non-technical means, as well as considering strictly defined 'cyber' operations and the relationship between the two.

Significantly, Ukraine also conceptualizes information security and cybersecurity as two complementary but interlinked areas of national security. This reflects both its partially shared tradition of defence and security thinking with Russia dating from Soviet times, and Ukraine's practical experience of persistent hostile cyber and information operations carried out by Russia since 1991.[5]

---

1 NATO's doctrine on targeting, for instance, refers to the integration of cognitive effects as 'still in its infancy'. See NATO (2021), *NATO Standard AJP-3.9: Allied Joint Doctrine for Joint Targeting*, Edition B, version 1, November 2021, https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/1033306/AJP-3.9_EDB_V1_E.pdf. In fact, use of this terminology appears to vary widely between NATO nations and within the organization itself. NATO's Defence Education Enhancement Programme (DEEP), for example, refers to cyber as 'an important field for information warfare', clearly placing it as a subset of information warfare in the same way as Russian doctrine. But this is far from universal. See NATO DEEP (undated), 'What is information warfare?', https://www.nato.int/nato_static_fl2014/assets/pdf/2020/5/pdf/2005-deepportal4-information-warfare.pdf.

2 Giles, K. (2016), *Handbook of Russian Information Warfare*, Fellowship Monograph, NATO Defense College, https://www.ndc.nato.int/news/news.php?icode=995.

3 Hakala, J. and Melnychuk, J. (2021), *Russia's Strategy In Cyberspace*, NATO Strategic Communications Centre of Excellence, https://stratcomcoe.org/cuploads/pfiles/Nato-Cyber-Report_11-06-2021-4f4ce.pdf; Cheravitch, J. (2021), *The Role of Russia's Military in Information Confrontation*, CNA, https://www.cna.org/reports/2021/06/The-Role-of-Russia%27s-Military-in-Information-Confrontation.pdf.

4 Encyclopedia of the Ministry of Defence of the Russian Federation (undated), 'Информационное противоборство' [Information confrontation], https://encyclopedia.mil.ru/encyclopedia/dictionary/details.htm?id=5221@morfDictionary.

5 See 'Cyber Security Strategy of Ukraine' (2018), available at https://ccdcoe.org/uploads/2018/10/NationalCyberSecurityStrategy_Ukraine.pdf. This compares to 'Doctrine of Information Security of Ukraine' (undated), available at https://rm.coe.int/doctrine-of-information-security-of-ukraine-developments-in-member-sta/168073e052.

Notes on this paper

This survey of Russian cyber and information warfare is based on reporting to the end of June 2023. It relies on open, publicly available sources. Additional context and background for the information gathered from open sources were provided by members of a multinational and multidisciplinary study group, who reviewed an early draft of the paper in April 2023 and contributed important corrections and clarifications.

Reliance on open sources places a clear caveat on the findings of this paper; not least because it is impossible to arrive at a complete and confident picture of cyber operations without access to telemetry, much of which is classified or confidential. A further caveat arises from the fact that there is a disparity between the effectiveness of operational security (OPSEC) practised by Ukraine and Russia respectively. The more effective nature of Ukraine's efforts to control information flows is evidenced in battlefield successes such as its launch of the Kharkiv counteroffensive in September 2022, to the apparent surprise of Russian forces as well as the world media. This also makes it difficult in many instances to determine the actual nature of cyber and information operations taking place in Ukraine, and close to impossible for outside observers to do so at the time they are taking place.

Although the author did not have access to specialized databases and repositories of information on cyber activities maintained by cybersecurity companies, the primary sources of information on cyber activity in the Ukraine theatre nevertheless remain public reporting by information and communications technology companies, rather than the Ukrainian state. The limits on what can be determined from open sources are illustrated by the way coverage of cyber activity in the early days of the invasion mirrored coverage of the air war in conveying the impression that nothing much was happening.[6] Because cyber and air operations were not visible to outside observers and did not play out in front of the world's media in the same manner as land operations did, it took time for the detail of what happened to emerge, leading to early descriptions of the conflict as a 'cyberwar that never was'.[7] In the case of air fighting, the true picture became clear in retrospective analysis and reconstructions by leading experts at defence think-tanks.[8] In the case of cyber operations, subsequent surveys and reports by entities such as Microsoft eventually described and explained what had taken place months before.[9]

Perceptions of impact can also be skewed by the fact that cyber operations in particular can remain effectively invisible to the public. As with espionage, some cyber operations are designed to remain undetected, but even those designed for

---

6 Bronk, J. (2022), 'The Mysterious Case of the Missing Russian Air Force', Commentary, RUSI, 28 February 2022, https://rusi.org/explore-our-research/publications/commentary/mysterious-case-missing-russian-air-force.
7 Gomez, M. A. (2022), 'The Cyberwar That Never Was: Reassessing Choices During Cyber Conflicts – Analysis', Eurasia Review, 17 July 2022, https://www.eurasiareview.com/17072022-the-cyberwar-that-never-was-reassessing-choices-during-cyber-conflicts-analysis.
8 Khan, I. (2023), 'The Aerial War Against Ukraine: The First Six Months', FOI Memo 8133, February 2023, Swedish Defence Research Agency, https://www.foi.se/rest-api/report/FOI%20Memo%208133; Bronk, J., Reynolds, N. and Watling, J. (2022), 'The Russian Air War and Ukrainian Requirements for Air Defence', RUSI, 7 November 2022, https://rusi.org/explore-our-research/publications/special-resources/russian-air-war-and-ukrainian-requirements-air-defence.
9 A detailed reconstructive chronology of cyber-related incidents affecting Ukraine is available at: National Security Archive, George Washington University (undated), 'Cyber Vault Ukraine Timeline', https://nsarchive.gwu.edu/document/29562-cyber-vault-ukraine-timeline.

palpable impact may remain unknown unless and until they succeed and damage or disruption is caused. Comprehensive reviews of operations in the first few months after February 2022 concluded that 'the modest scale of Russia's cyberattacks has fallen far short of … predictions'[10] and consequently that 'cyber has not been a consequential front in Russia's invasion of Ukraine'.[11] However, as later explained by Sir Jeremy Fleming, the outgoing chief of the UK's Government Communications Headquarters (GCHQ) signals intelligence agency, 'There's been plenty of cyber in this conflict. The thing that's different is … that Ukraine has been very effective in defending itself.'[12] It has thus taken time for a clearer picture of the cyber and information aspects of the war to emerge.

By the time this paper was substantively complete in August 2023, however, despite gaps in visibility into specific technical aspects of cyber operations there was sufficient verifiable reporting on incidents across the entirety of information confrontation to arrive at a number of confident findings on how this conflict had confirmed, or run counter to, prior expectations.

The nature of the conflict

Ahead of 24 February 2022, there was a widespread expectation of a swift and devastating campaign by crushingly superior Russian forces. This did not take place, either in conventional or in cyber and information operations. This came as a considerable surprise to many commentators around the world who had not observed the way in which Ukraine's military and information capacity had developed during the preceding eight years since Russia's seizure of Crimea and initial invasion of eastern Ukraine. Fortunately for Ukraine, developments in the early stages of the full-scale 2022 invasion also came as a considerable surprise to Russia's own armed forces and planners. This influenced the evolution of Russia's cyber and information campaign over the subsequent months of war.

While Russia's conventional military performance in Ukraine has been studied extensively, there are also lessons on capability and future conflict with Russia to be drawn from Russia's cyber and information warfare campaigns. Just as in conventional warfare, events in Ukraine have triggered a substantial rethink of Russia's real, as opposed to claimed, capabilities.[13] Earlier analysis on this theme by respected colleagues and institutions working in this field is referenced throughout this paper.

Crucially, in information space, unlike in other domains, Russia's lack of early success in Ukraine appeared *not* to have resulted from failures to implement doctrine and planning. Russia attempted precisely the types of cyber and information attack that it had been practising and developing over the preceding years, as described

---

10 Kostyuk, N. and Gartzke, E. (2022), 'Why Cyber Dogs Have Yet to Bark Loudly in Russia's Invasion of Ukraine', *Texas National Security Review*, 5(3), pp. 113–26, Summer 2022, https://tnsr.org/2022/06/why-cyber-dogs-have-yet-to-bark-loudly-in-russias-invasion-of-ukraine.
11 Soldatov, A. and Borogan, I. (2022), *Russian Cyberwarfare: Unpacking the Kremlin's Capabilities*, Center for European Policy Analysis (CEPA), https://cepa.org/russian-cyberwarfare-unpacking-the-kremlins-capabilities.
12 Khalaf, R. (2023), 'GCHQ's Jeremy Fleming: "Xi doesn't want to see Putin humiliated"', *Financial Times*, 26 May 2023, https://www.ft.com/content/7979924f-dfa3-4da2-adda-23c1dceda41c.
13 Dalsjö, R., Jonsson, M. and Norberg, J. (2022), 'A Brutal Examination: Russian Military Capability in Light of the Ukraine War', *Survival*, 63(3), pp. 7–28, https://doi.org/10.1080/00396338.2022.2078044.

in multiple specialist publications both within Russia and beyond. These types of attack included information interdiction, personalized targeted deception delivered to connected devices, selective destruction of civilian telecommunications infrastructure, and attempts at integration of kinetic and cyber/information activity.[14]

While Russia's conventional military performance in Ukraine has been studied extensively, there are also lessons on capability and future conflict with Russia to be drawn from Russia's cyber and information warfare campaigns.

However, many of these activities did not succeed, and other anticipated campaigns did not materialize. For example, large-scale and successful destructive cyberattacks on critical infrastructure were widely anticipated as a key element of swift Russian victory.[15] Instead, Ukraine has largely prevailed against such attacks to date, and many of the apparent aims of Russian cyber and information activity have not been met. How and why this happened, and what this can tell us for planning of defence against Russia's next war, is a major theme throughout this paper.

After consideration of the initial phase of Russia's full-scale invasion of Ukraine in February 2022 and the underlying principles of successful Ukrainian resistance to information confrontation that this revealed, the paper has four main chapters. First, it considers those features of information confrontation that appear to be new and distinctive in this conflict. Second, it surveys the specific aspect of cognitive warfare – the battle for perceptions in pursuit of tactical, operational or strategic aims – as demonstrated in Ukraine itself, in and against Russia, and across the rest of the world. Third, the paper presents a summary of lessons observed that are pertinent to Western nations' planning for future conflict. The paper concludes with a set of specific policy recommendations for Western governments and coalitions that might seek to defend themselves against Russian information confrontation methods and capabilities in the future.

---

14 According to a formal British definition, 'Kinetic effects are achieved by projectiles of some kind hitting a target and leading to tangible destruction.' See UK Parliament (2004), *House of Commons Select Committee on Defence Fifth Report*, 23 June 2004, https://publications.parliament.uk/pa/cm200304/cmselect/cmdfence/465/46507.htm.
15 Miller, M. (2022), 'Russian invasion of Ukraine could redefine cyber warfare', Politico, 28 January 2022, https://www.politico.com/news/2022/01/28/russia-cyber-army-ukraine-00003051.

02 Ukrainian resilience and resistance in 2022

Just as with conventional military operations, Ukraine's unexpected resilience to information warfare campaigns and cyberattack confounded Russian expectations and assumptions in the early phases of the full-scale war. But many assumptions by foreign observers were also misplaced.

Opening salvoes

Just as with assessments of Russian conventional warfare against Ukraine, there is a broad consensus in analysis of the early stages of Russia's cyber campaign against its neighbour in 2022 that the forces waging it were fundamentally unprepared for the nature of the conflict that developed.

In some analysis, this has been attributed to Russia's cyber forces being as uninformed as the ground troops on overall plans to launch the invasion, and being given no time to prepare for the new nature of the conflict.[16] This, however, is not borne out by other observations, which suggest that those involved in cyber and information activities – like the rest of the Russian military and intelligence services – were prepared for a swift 'special military operation' but were startled by it turning into a full-scale war in which the enemy fought back.

16 Sakellariadis, J. and Miller, M. (2023), 'Ukraine gears up for new phase of cyber war with Russia', Politico, 25 February 2023, https://www.politico.com/news/2023/02/25/ukraine-russian-cyberattacks-00084429.

Activities before and during the initial stages of the assault suggest that Russia's cyber and information forces were better prepared than its armour and infantry. A spike in destructive cyber assaults against Ukraine occurred in January and February 2022, and has been characterized in one analysis as a process of 'softening up by software'.[17] Attacks that sought to suppress communications by Ukraine's government and military indicate that long-term, coordinated preparation was involved. One example was the attack on the Viasat KA-SAT network immediately before 24 February, which was followed up by conventional and electronic warfare (EW) attacks also designed to blind Ukrainian forces.[18] The clearest evidence of Russia's information preparations for the move into Ukraine came in the execution of plans to round up previously identified individuals as soon as Russian forces gained control of a particular city or town.[19] In keeping with consistent practice during Soviet times, arrests, interrogations and murders of public servants, politicians, local activists, journalists, police officers, war veterans and other groups were an immediate priority.[20] Russian forces were fully equipped with lists of names, telephone numbers and addresses of those to look for.[21]

But it is likely that failure to anticipate Ukrainian resistance severely impaired other cyber and information operations intended to support Russia's conventional war effort. In the early stages of the new invasion, further destructive attacks on communications and other infrastructure were constrained by an assumption that Ukraine would fall without a fight, and that infrastructure would be taken over by Russian authorities. Once that assumption was discovered to be distant from reality, Russia's forces across the board found themselves fighting an unanticipated war. This may have contributed to a further transition in the ensuing months, when there was a change in tempo to what have been described as 'fast and dirty' cyber methods,[22] as Russian cyber forces transitioned to tactics that required less forward planning and were more straightforward to implement; these included distributed denial of service (DDoS) attacks and the deployment of a new generation of less sophisticated and modular 'wiper' malware.[23]

Analysis from December 2022 concluded: 'Russia's experience suggests that cyber fires can be usefully concentrated in a surprise attack or other major salvo, but they risk fading in relevance during larger, longer wars.'[24] This seems

---

17 *The Economist* (2022), 'Lessons from Russia's cyber-war in Ukraine', 30 November 2022, https://www.economist.com/science-and-technology/2022/11/30/lessons-from-russias-cyber-war-in-ukraine.
18 Another posited explanation is that this was possible on the basis of available contingency planning without forewarning, since the unique transitory nature of cyber weapons necessitates constant preparatory cycles – as described in Smeets, M. (2017), 'A matter of time: On the transitory nature of cyberweapons', *Journal of Strategic Studies*, 41(1–2), pp. 6–32, https://doi.org/10.1080/01402390.2017.1288107.
19 Bajak, F. (2022), 'A chilling Russian cyber aim in Ukraine: Digital dossiers', AP, 28 April 2022, https://apnews.com/article/russia-ukraine-technology-business-border-patrols-automobiles-fa3f88e07e51bcaf81bac8a40c4da141.
20 Watling, J., Danylyuk, O. V. and Reynolds, N. (2023), 'Preliminary Lessons from Russia's Unconventional Operations During the Russo-Ukrainian War, February 2022–February 2023', RUSI, 29 March 2023, https://rusi.org/explore-our-research/publications/special-resources/preliminary-lessons-russias-unconventional-operations-during-russo-ukrainian-war-february-2022. See also the sources in footnotes 19 and 21.
21 Kinetz, E. (2022), '"We Will Find You:" Russians Hunt Down Ukrainians on Lists', PBS, 21 December 2022, https://www.pbs.org/wgbh/frontline/article/russians-hunt-down-ukrainians-on-lists; Chappell, B. (2022), 'The U.S. warns that Russia has a 'kill list' of Ukrainians to be detained or killed', NPR, 21 February 2022, https://www.npr.org/2022/02/21/1082096026/russia-kill-list-ukraine.
22 Greenberg, A. (2022), 'Russia's New Cyberwarfare in Ukraine Is Fast, Dirty, and Relentless', WIRED, 10 November 2022, https://www.wired.com/story/russia-ukraine-cyberattacks-mandiant.
23 Sakellariadis and Miller (2023), 'Ukraine gears up for new phase of cyber war with Russia'.
24 Bateman, J. (2022), *Russia's Wartime Cyber Operations in Ukraine: Military Impacts, Influences, and Implications*, Carnegie Endowment for International Peace, 16 December 2022, https://carnegieendowment.org/2022/12/16/russia-s-wartime-cyber-operations-in-ukraine-military-impacts-influences-and-implications-pub-88657.

to contradict another key aspect of Russia's employment of information and cyber effects, namely that 'the demands of preparation for a combined-arms campaign do not lend themselves well to Moscow's more nebulous notions of information warfare as an ongoing, unending struggle'.[25] However, both of these assessments can be valid at once due to the specific view held by Russia and other nations of information warfare as a holistic activity, in which cyber campaigning is simply a manifestation of information manipulation. One practical result for Russia's armed forces is the continuing need to integrate cyber effects with conventional warfare at an operational and tactical level, as well as treating them as strategic tools. This was one of the intents behind the establishment of Russia's 'Information Operations Troops';[26] and it has led to a distinctive structure for this element of Russia's armed forces, grouped under the GRU military intelligence service.[27] Importantly, Russia sees cyber operations in wartime not as a direct replacement for missiles and bombs for destructive effect (as interpreted in some popular Western descriptions), but as applicable to far more uses.

One result of the war developing in an unexpected direction appears to have been unanticipated demands on Russia's cyber forces which they may have been poorly prepared to meet, due to a lack of forward planning appropriate to a protracted conflict.[28] This may have led to early squandering of advantages held by Russia. Google's Threat Analysis Group notes that the destructive impact of attacks on Ukrainian networks around the time of the full-scale invasion was not as significant as that of earlier Russian cyber campaigns against Ukraine, and that the attacks wasted access gained months in advance. The expectation of a short war led to a 'lack of operational preparation that could have sustained some persistent accesses while burning others during destructive activity', Google concluded.[29]

Preconditions for Ukrainian resilience

One simple fact working against Russia was that its war on Ukraine did not in fact start on 24 February 2022. Expectations of cyber and cyber-enabled effects that would leverage an adversary's surprise and unpreparedness were misplaced. Although Russia might have been expected to take a different operational approach in full-scale conflict compared to the limited warfare waged in 2014–22, the preceding eight years of hostilities nevertheless gave Ukraine ample time to study Russia's capabilities and intentions and develop resilience. Ukraine's

---

25 Wilde, G. (2022), *Cyber Operations in Ukraine: Russia's Unmet Expectations*, Carnegie Endowment for International Peace, 12 December 2022, https://carnegieendowment.org/2022/12/12/cyber-operations-in-ukraine-russia-s-unmet-expectations-pub-88607.
26 Giles, K. (2011), 'Information Troops – a Russian Cyber Command?', in Czosseck, C. et al. (eds) (2011), 3rd International Conference on Cyber Conflict, http://195.222.11.251/uploads/2018/10/InformationTroopsARussianCyberCommand-Giles.pdf.
27 A purported order of battle for the GRU's Information Operations Troops can be found at 'Центры информационных операций ГРУ ГШ в ваших руках' [The GRU information operations centres are in your hands], Sliv, 22 July 2022, https://sliv.top/2022/07/22/czentry-informaczionnyh-operaczij-gru-gsh-v-vashih-rukah.
28 Kostyuk and Gartzke (2022), 'Why Cyber Dogs Have Yet to Bark Loudly in Russia's Invasion of Ukraine'.
29 Google Threat Analysis Group (2023), 'Fog of war: how the Ukraine conflict transformed the cyber threat landscape', 16 February 2023, https://services.google.com/fh/files/blogs/google_fog_of_war_research_report.pdf.

cyber defences, like its armed forces, had developed beyond recognition from their threadbare and compromised state in 2014[30] – although this development too was widely underestimated outside Ukraine itself.

An additional enabler for Ukraine was support from abroad, both nationally and by private industry. In the lead-up to the invasion, Google observed the pattern of attacks against Ukrainian media and civil society websites and decided to extend its Project Shield protection against DDoS attacks – first to the *Ukrainska Pravda* news website, and then to a further 2,300 sites judged to be important to keep functioning. This meant that when major attacks were mounted against these sites, they were in a form that would have been overwhelming for an individual site but were trivial for a network and capabilities on the scale of Google's. This, too, reputedly caused surprise on the Russian side. According to one account: 'Folks in the Kremlin pressed the button with glee. Then nothing happened – so they pressed it again.'[31] The nature and impact of the foreign support provided to Ukraine will be examined in detail later in this paper.

Social media platforms operating by peacetime norms can be deeply unhelpful to a country fighting a war of national survival.

Other technology companies, however, were less cooperative. As Ukraine has found with Facebook suppressing commentary on Russian actions, and not responding to investigative enquiries into hostile information operations in a timely manner, social media platforms operating by peacetime norms can be deeply unhelpful to a country fighting a war of national survival.[32] Ukraine's efforts at maintaining the integrity of its own information space were also hampered by the fact that the regional headquarters of many technology companies were in Russia, not Ukraine.[33] The Google office making decisions on content carried by Google's YouTube platform for Ukraine was in St Petersburg, and Ukrainian information professionals noted repeated instances of undue promotion of pro-Russian content on the platform. They have noted that Apple, too, ran its Ukrainian operations from Russia, meaning that hardware was distributed through Moscow and consequently implying that the FSB – Russia's Federal Security Service – potentially had access to smartphones before these reached the Ukrainian market, thus potentially compromising their security. Similarly, companies like HP and Cisco also covered Ukraine from Moscow, meaning that technical data for the country was routed through Russia and thus vulnerable to access by the Russian intelligence services. Consequently, it was impossible to build network infrastructure that would be inherently secure.

---

30 Geers, K. (2015), *Cyber War in Perspective: Russian Aggression against Ukraine*, NATO Cooperative Cyber Defence Centre of Excellence, https://ccdcoe.org/uploads/2018/10/CyberWarinPerspective_full_book.pdf.
31 A senior executive at a major Western technology company, speaking under the Chatham House Rule, Tallinn, 12 May 2023.
32 Spriņģe, I. (2023), 'Does Facebook Censor Posts in Support of Ukraine?', re:Baltica, 7 March 2023, https://en.rebaltica.lv/2023/03/does-facebook-censor-posts-in-support-of-ukraine.
33 It should be noted that 'integrity of national information space', a key enabler for resilience to external attack, is a core element of Russian conceptualization of information confrontation but conflicts with Western notions of a free and global internet. See Drazdovich, U. (2023), 'Words and Actions: Understanding Russia's Information Security Strategy', master's thesis, Harvard University Division of Continuing Education, May 2023, https://nrs.harvard.edu/URN-3:HUL.INSTREPOS:37374936.

As noted above, Ukrainian OPSEC measures have been highly effective. One result of this is a dearth of reporting on successful information operations by Russia – or on other forms of setback or failure by Ukraine. Reporting of this kind, when not easily dismissed as Russian hyperbole, can be difficult to confirm, so there are only isolated descriptions from authoritative sources suggesting that cyber or cyber-enabled operations may have had a substantial impact on Ukrainian battlefield capability. For instance, in the earliest phases of the conflict, Bayraktar TB-2 unmanned aerial vehicles (UAVs) were a significant asset for Ukraine (albeit widely hyped in information campaigns); but they later virtually disappeared from the battlefield.[34] This could be explained by developments in Russia's air defence posture from the early and chaotic days of the invasion, but Google attributes this to a successful act of cyber espionage by Russia's FrozenBarents/Sandworm cyber operations group on the drones' Turkish manufacturer, which enabled Russian forces to discover means to disable them.[35] (A more prosaic possible explanation is that during this period Bayraktars were also supplied to the Russia-friendly government of Mali, which could well have passed on observations on best practice for neutralizing them.)[36] Meanwhile, multiple sources note that other campaigns have targeted sensitive information like Ukrainian military communications and troop movements – but these sources have not provided the kind of detail that would allow an assessment of how such targeting was carried out, what the effect was, and whether this provides transferable lessons for other conflicts.[37]

The fact that cellular telecommunications networks need to stay up and are used by both Ukrainian and Russian troops, at times for operational as well as personal purposes, has been exploited by both sides.[38] The apparent asymmetric success enjoyed by Ukraine in this field once again derives not only from defensive countermeasures but also from a significant difference in operational security. Russia's poor OPSEC has led both to extensive communications intercepts and to effective exploitation of the information in them, whereas in relative terms genuine Russian intercepts of Ukrainian conversations seem to have been almost non-existent. But in addition, here too Russia is using familiar techniques delivered by systems that have been well known for years, such as the Leer-3 UAV-borne EW system for harvesting data from and disseminating content to an adversary's connected devices.[39] These are, again, methods with which Ukraine's forces had grown familiar over an extended period prior to the full-scale invasion in February 2022, and so these techniques had limited potential to deliver decisive new impact.

---

34 Dangwal, A. (2022), 'Bayraktar TB2 Drones 'Out Of Action' From Ukraine War; Russia's Air Defense Or Diplomacy Behind Their Disappearance?', *EurAsian Times*, 4 December 2022, https://eurasiantimes.com/bayraktar-tb2-drones-out-of-action-from-ukraine-war-russias.
35 Google Threat Analysis Group (2023), 'Fog of war: how the Ukraine conflict transformed the cyber threat landscape'.
36 Lionel E. (2023), 'Mali receives additional L-39C Albatros and Bayraktar TB2', Military Africa, 17 March 2023, https://www.military.africa/2023/03/mali-receives-additional-l-39c-albatros-and-bayraktar-tb2.
37 See, for instance, Antoniuk, D. (2023), 'Ukraine says it thwarted attempt to breach military tablets', Recorded Future, 8 August 2023, https://therecord.media/ukraine-military-tablets-sandworm-hacking-attempt.
38 Devine, K. (2023), 'Ukraine war: Mobile networks being weaponised to target troops on both sides of conflict', Sky News, 4 January 2023, https://news.sky.com/story/ukraine-war-mobile-networks-being-weaponised-to-target-troops-on-both-sides-of-conflict-12577595.
39 Giles, K. (2015), 'The Next Phase of Russian Information Warfare', NATO Strategic Communications Centre of Excellence, https://stratcomcoe.org/publications/the-next-phase-of-russian-information-warfare/176.

Ukraine's successful efforts at crowdsourcing resistance – making best use of the volunteer services of a population highly motivated to fight a war of national survival – have been reported on extensively.[40] These have included effective tasking of the entire civilian population for intelligence collection and reporting (the legal implications of which are also discussed further below).[41] Resilience measures have also involved the specific and careful preparation of decision-makers in government and industry as well as other stakeholders. Focused efforts at building networks, ensuring communications and gaming out crisis cooperation through table-top exercises in the months before Russia's escalation helped prepare key leaders for the reality of conflict.

The overall effect of these combined measures has been to keep the Ukrainian state largely functioning online, despite Russia's best efforts to prevent it from doing so. Success in this regard can be measured against other countries in the region and beyond: Ukraine daily withstands numerous attacks on a scale that has proven capable of taking entire governments offline in countries that have invested less in their resilience.[42]

40 Husarska, A. (2023), 'Ukrainian Engineers, Historians and Housewives Are Keeping Putin on His Toes', *New York Times*, 12 January 2023, https://www.nytimes.com/2023/01/12/opinion/ukraine-war.html.
41 Smith-Boyle, V. (2022), 'How OSINT Has Shaped the War in Ukraine', American Security Project, 22 June 2022, https://www.americansecurityproject.org/osint-in-ukraine.
42 Cybersecurity & Infrastructure Security Agency (CISA) (2022), 'Iranian State Actors Conduct Cyber Operations Against the Government of Albania', 23 September 2022, https://www.cisa.gov/news-events/cybersecurity-advisories/aa22-264a.

03 Distinctive features of the war

Cyber and information operations in Ukraine have displayed a number of novel features alongside tried and familiar Russian tactics. Notably, private industry and individuals have been directly engaged in combat support for Ukraine, raising questions over their legal status.

State and commercial support for Ukraine

State support

At a state level, formal cybersecurity cooperation arrangements are in place between Ukraine and the US,[43] and direct support in cyber operations by Western governments has been confirmed, although its nature remains understandably opaque. Canada is providing direct cybersecurity support to Ukraine as well as to Latvia, where Canada is the framework nation for NATO's 'Enhanced Forward Presence' deployment. Designating both Ukrainian and Latvian networks as 'systems of importance' to the Canadian government mandates the provision of ongoing state assistance.[44] Canada is also supporting satellite communications services in Ukraine to help maintain continuity of critical cyber systems.[45] Paul Chichester, director of operations at the UK's National Cyber Security Centre (NCSC), has described defending Ukraine's networks as the 'primary mission' for both global private sector companies and British government cybersecurity

43 CISA (2022), 'United States and Ukraine Expand Cooperation on Cybersecurity', 27 July 2022, https://www.cisa.gov/news/2022/07/27/united-states-and-ukraine-expand-cooperation-cybersecurity.
44 Tunney, C. (2023), 'Canada quietly extended its cyber defence umbrella to Ukraine, Latvia after Russian invasion: report', CBC News, 29 June 2023, https://www.cbc.ca/news/politics/defence-cyber-ukraine-latvia-canada-1.6892420.
45 Communications Security Establishment (2023), 'Communications Security Establishment Annual Report 2022-2023', https://www.cse-cst.gc.ca/en/accountability/transparency/reports/communications-security-establishment-annual-report-2022-2023.

agencies.[46] The head of US Cyber Command, General Paul Nakasone, has confirmed that the US has 'conducted a series of operations across the full spectrum; offensive, defensive, [and] information operations'[47] – although 'offensive cyber operations' were left undefined and thus potentially referred to activities ranging widely in nature, scale and impact.[48] This support and the essential mutual trust it requires appeared to recover swiftly from the abrupt withdrawal from Ukraine of embedded foreign cyber support personnel, along with other military trainers from the US, UK and Canada, ahead of the invasion in February 2022.[49]

At a state level, formal cybersecurity cooperation arrangements are in place between Ukraine and the US, and direct support in cyber operations by Western governments has been confirmed, although its nature remains understandably opaque.

Not all foreign support is the result of new measures following February 2022; some international support programmes were in place years beforehand.[50] US Cyber Command deployed its largest 'hunt forward' package – an operation to examine and strengthen a partner nation's networks – to date to Kyiv in early December 2021.[51] According to Anne Neuberger, deputy national security adviser for cyber and emerging technology in the US National Security Council: '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.'[52] Other direct support measures date back much further. NATO's 'Cyber Defence Trust Fund', established after the NATO summit in Wales in 2014, was designed to develop Ukrainian capabilities to counter cyberthreats.[53] 'EU4Digital: Cybersecurity East' was an analogous project run by the EU since 2019.[54] A US assistance package delivered through the USAID agency since 2020 has focused on the cybersecurity of critical infrastructure. As ever, the precise extent and practical effect of each

46 Martin, A. (2022), 'Ukraine war: US cyber chief on Kyiv's advantage over Russia', Sky News, 8 June 2022, https://news.sky.com/story/ukraine-war-us-cyber-chief-on-kyivs-advantage-over-russia-12628869.
47 Martin, A. (2022), 'US military hackers conducting offensive operations in support of Ukraine, says head of Cyber Command', Sky News, 1 June 2022, https://news.sky.com/story/us-military-hackers-conducting-offensive-operations-in-support-of-ukraine-says-head-of-cyber-command-12625139.
48 Zetter, K. (2022), 'What It Means that the U.S. Is Conducting Offensive Cyber Operations Against Russia', Zero Day, 17 June 2022, https://zetter.substack.com/p/what-it-means-that-the-us-is-conducting.
49 Corera, G. (2022), 'Inside a US military cyber team's defence of Ukraine', BBC News, 30 October 2022, https://www.bbc.co.uk/news/uk-63328398.
50 Chertoff, M. and Kaushik, A. (2023), 'The unheralded success story of Ukraine's cyber-defences', EUObserver, 1 March 2023, https://euobserver.com/opinion/156766.
51 Banco, E. et al. (2023), "Something Was Badly Wrong': When Washington Realized Russia Was Actually Invading Ukraine', Politico, 24 February 2023, https://www.politico.com/news/magazine/2023/02/24/russia-ukraine-war-oral-history-00083757.
52 Ibid.
53 NATO (2015), 'NATO's practical support to Ukraine', Fact Sheet, December 2015, https://www.nato.int/nato_static_fl2014/assets/pdf/pdf_2015_12/20151130_1512-factsheet-nato-ukraine-supportr_en.pdf.
54 EU4Digital website at https://eufordigital.eu/discover-eu/eu4digital-improving-cyber-resilience-in-the-eastern-partnership-countries.

of these programmes are unquantifiable without detailed insider knowledge, but their cumulative impact is widely credited with having transformed Ukraine's defensive capabilities and resilience to cyber campaigns.

Private industry support

In addition to support provided at a national level, a wide spectrum of technology companies is providing an equally wide range of essential services in support of Ukraine. Imagery from commercial satellites has been a critical enabler for the Ukrainian war effort, not only contributing to situational awareness but shaping the narratives of the war. In response, Russia has reportedly adopted temporary and reversible countermeasures, such as jamming and non-destructive cyberattacks against satellite services.[55] Support from Amazon and its cloud services was crucial in evacuating Ukrainian government data from fixed premises.[56] This was a last-minute measure carried out shortly before the February 2022 invasion, but one with a clear precedent in other countries that consider themselves at risk of being overrun by Russian forces, as in the case of Estonia setting up overseas 'data embassies' in the previous decade.[57] Microsoft and ESET, a digital security company, have been identified as particularly useful in facilitating cyber defence due to their pervasive presence on Ukrainian networks. This assists with situational awareness and the collection of telemetry which is then passed to Ukrainian authorities, complementing direct responses in the form of building protections against detected threat activity into software products so that not only Ukrainian customers but others worldwide can benefit. Google is providing support services for Ukrainian government functions as well as DDoS protection for government websites and embassies worldwide. The Cyber Defense Assistance Collaborative (CDAC), a coalition of service providers, is delivering assistance *pro bono* or funded by non-governmental philanthropic grants.[58] Meanwhile, companies such as Microsoft, Google and Amazon have provided services either at their own cost, or funded by Western governments backing Ukraine – albeit while issuing occasional reminders of the cumulative financial value of the support they have provided to date.

Appreciation of the role and power that major technology companies have in modern conflict may vary between organizations. But there are constraints that are largely common to many of them, connected with the need to meet obligations to shareholders and boards and comply with regulatory regimes, both locally and at their global headquarters. While corporations routinely show greater agility than governments do, legal and organizational constraints on corporate action still inform decisions. Most corporations will also need to justify policy decisions such as taking sides in a conflict to their own workforces, in order to prevent internal disruption.

---

55 Erwin, S. (2022), 'Drawing lessons from the first 'commercial space war'', SpaceNews, 20 May 2022, https://spacenews.com/on-national-security-drawing-lessons-from-the-first-commercial-space-war.
56 Mitchell, R. (2022), 'How Amazon put Ukraine's 'government in a box' – and saved its economy from Russia', *Los Angeles Times*, 15 December 2022, https://www.latimes.com/business/story/2022-12-15/amazon-ukraine-war-cloud-data.
57 Techerati (2016), 'Estonia will create overseas 'data embassy'', 25 July 2016, https://www.techerati.com/the-stack-archive/data-centre/2016/07/25/estonia-will-create-overseas-data-embassy.
58 CRDF Global (2022), 'CRDF Global becomes Platform for Cyber Defense Assistance Collaborative (CDAC) for Ukraine', PR Newswire, 14 November 2022, https://www.prnewswire.com/news-releases/crdf-global-becomes-platform-for-cyber-defense-assistance-collaborative-cdac-for-ukraine-301676373.html.

The issue of cost does not appear yet to have stopped any technology company from providing necessary support to Ukraine, but the question remains of how long this is sustainable. While the major players are large enough to write off the costs of support without significant financial impact, this does not apply across the industry, especially if support turns into a multi-year commitment. Eventually, shareholder discontent could have a significant impact on critical service provision for Ukraine.

Companies will have learned from the experience of Ukraine that they need strategies and pre-agreed policies to cover the possibility that commitments turn out to be far more prolonged and costlier than anticipated.

Companies the size of Microsoft, for example, have dedicated disaster response divisions set aside for emergency or humanitarian contingencies. These departments could be considered the natural sources of corporate action in support of a victim of aggression. But with or without specific disaster response capabilities, companies will have learned from the experience of Ukraine that they need strategies and pre-agreed policies to cover the possibility that commitments turn out to be far more prolonged and costlier than anticipated. This is particularly the case because it would most likely be reputationally challenging for a company to withdraw critical support in mid-war. Support for a combatant also exposes corporations to the legal implications of being a party to the conflict, discussed further below.

In fact, rather than conforming to notions of warfare that takes place between states using national resources, the cyber and information aspects of the current conflict are heavily dependent on private commercial organizations. Providers of cybersecurity services, network components, software, cloud services and much more are all directly involved. And the embedding of the private sector in Ukraine's information systems provides a warfighting advantage unique to this domain: when the enemy deploys a new weapon system (the cyber equivalent being, for instance, malware), that system can on occasion be identified and mitigated or neutralized at far greater speed than in conventional operations, and by organizations other than the state. A by-product of this syndrome is that private industry may have better situational awareness than governments, especially those that – unlike industry – are not directly party to the conflict. While no individual entity has overall visibility of what is happening in Ukraine or any other cyber conflict, the combined effect of industry insights into overlapping segments of networks or industries provides clarity that may not be directly available to state actors.

Overall, a transformative effect of the situation in Ukraine has been to improve the exchange of information and foster apparent deconfliction between notional competitors in the cyber and information technology industries. While competitiveness between major technology companies prevents full strategic cooperation, a shared sense of purpose sees them to some extent working together against a common threat in the same way that the coalition of states backing Ukraine

cooperates to pool and share resources for best effect. Here, too, the distinction in behaviour between large corporations and states appears to be eroding. According to Microsoft's president, Brad Smith, the process of getting involved in geopolitics was 'unusual and even uncomfortable, but became indispensable for the protection of our customers'.[59] The net result is that, to an unprecedented degree, 'the conduct of war and other responsibilities in the realm of statehood are reliant on private actors'.[60]

At present, those organizations have largely decided which side they are on; but in a future, more ambiguous conflict, their loyalties could span borders and they could find themselves offering services to both sides. Their own commercial exposure could be an additional determining factor. In a future conflict involving China, for example, consideration of potential loss of business as a result of backing the other side could be decisive. This has direct implications for future conflict. The capabilities of private sector security firms are an integral part of the cyber defence capability of Western states. The digital security of critical infrastructure, in particular, has largely been entrusted to private industry. This leaves open the questions of who is going to pay for the services of private technology companies when they are called on, and how to ensure that companies are going to be on the 'right' side – as opposed to neutral or even hostile.

Lessons from Starlink's involvement in Ukraine

Of all the forms of foreign support provided to Ukraine, few have had such a visibly transformative effect as the Starlink satellite communications service, offered to Ukraine shortly after the full-scale invasion.[61] A Ukrainian deputy prime minister, Olga Stefanishyna, has called the provision of Starlink services 'a turning point in our survival'. However, the evolution of the Ukrainian Armed Forces' relationship with Starlink also illustrates core problems of dependence on the private sector for defence capability – problems that go far beyond the context of Ukraine. In fact, given the nature and ownership of Starlink's parent company, SpaceX, this crucial capability was dependent not just on a single company but on one man; and in this case, a man renowned for his mercurial nature.[62]

Public frictions between Elon Musk and the Ukrainian government first arose over the issue of cost. A sudden realization in late 2022 that Starlink services could be abruptly withdrawn was deeply alarming for Ukraine, given the country's already well-established dependence on them; the dispute was then exacerbated by Andriy Melnyk, then serving as Ukrainian ambassador to Germany, responding to a 'peace proposal' by Musk with public profanity.[63] The fact that a fighting force could come

---

59 Prescott, K. (2022), 'Microsoft boosts digital aid for Ukraine', *The Times*, 4 November 2022, https://www.thetimes.co.uk/article/90818582-5ba0-11ed-9b1f-f7c251e9dfdc.
60 Schroeder, E. and Dack, S. (2023), 'A parallel terrain: Public-private defense of the Ukrainian information environment', Atlantic Council, 27 February 2023, https://www.atlanticcouncil.org/in-depth-research-reports/report/a-parallel-terrain-public-private-defense-of-the-ukrainian-information-environment.
61 Iyengar, R. (2022), 'Starlink Ukraine: Why Elon Musk Is the Go-To Internet Provider', *Foreign Policy*, 22 November 2022, https://foreignpolicy.com/2022/11/22/ukraine-internet-starlink-elon-musk-russia-war.
62 Farrow, R. (2023), 'Elon Musk's Shadow Rule', *New Yorker*, 21 August 2023, https://www.newyorker.com/magazine/2023/08/28/elon-musks-shadow-rule.
63 Marquardt, A. (2022), 'Exclusive: Musk's SpaceX says it can no longer pay for critical satellite services in Ukraine, asks Pentagon to pick up the tab', CNN, 14 October 2022, https://edition.cnn.com/2022/10/13/politics/elon-musk-spacex-starlink-ukraine/index.html.

to rely on a service which, it appeared, could simply be withdrawn by its owner at zero notice provides warnings for Western defence forces considering their future relationships with the private sector.

Starlink, although not designed as a military system, has features that were favourable for its adoption for military purposes. These include the phased array that reduces the need for physical alignment of the terminal and focuses signals in a tight beam, thus making the terminals harder to locate using EW means; the very high number of satellites in orbit, which renders jamming more challenging; and Starlink's combination of high bandwidth, low latency, small size and mobility.[64]

But the fact that this is a commercial service also carries drawbacks. 'Geofencing' – the limitation of service provision within virtual perimeters – meant that in October 2022, when advancing Ukrainian forces entered newly liberated areas, Starlink abruptly ceased to function, depriving those forces of critical communications capability at a vulnerable moment.[65] In the absence of definitive comment from Starlink, it remains unclear whether this was a deliberate limitation on Ukrainian use or a measure specifically designed to prevent the use of captured terminals by Russian forces.[66] In addition, more recent reporting suggests that Russian forces have developed means of targeting Starlink terminals, greatly increasing the vulnerability of users.[67]

In February 2023, Starlink placed further restrictions on usage, saying the system should not be used for offensive purposes such as providing communications for controlling drones carrying out attacks on Russian troops.[68] Rather than an attempt specifically to hobble or constrain Ukrainian operations and favour Russia, as suspected by some of the more hawkish of Ukraine's public backers, the restrictions were presented by Starlink as a response to an unanticipated expansion of its uses, from communications in general to specifically enabling offensive operations.[69] It is possible that an unspoken consideration was Starlink's unwillingness to expose itself to greater risk through becoming a direct party to attacks on Russian forces and assets, following Russian threats of countermeasures against private entities that did so – threats that, while so far empty, unusually had an arguable basis in international law. The lessons for private sector engagement elsewhere were again clear: a vital warfighting capability can be made unavailable on the basis of a terms-of-service violation.[70] This is a critically important issue: given the extent of Ukrainian reliance on support from the commercial sector,

---

64 Erwin, S. (2023), 'Limits on Ukraine's use of Starlink for war operations is a lesson for U.S. military', SpaceNews, 9 March 2023, https://spacenews.com/limits-on-ukraines-use-of-starlink-for-war-operations-is-a-lesson-for-u-s-military.
65 Srivastava M., Olearchyk, R., Schwartz, F. and Miller, C. (2022), 'Ukrainian forces report Starlink outages during push against Russia', *Financial Times*, 7 October 2022, https://www.ft.com/content/9a7b922b-2435-4ac7-acdb-0ec9a6dc8397.
66 Erwin (2023), 'Limits on Ukraine's use of Starlink for war operations is a lesson for U.S. military'.
67 Skove, S. (2023), 'Using Starlink Paints a Target on Ukrainian Troops', Defense One, 23 March 2023, https://www.defenseone.com/threats/2023/03/using-starlink-paints-target-ukrainian-troops/384361.
68 Marquardt, A. and Fisher, K. (2023), 'SpaceX admits blocking Ukrainian troops from using satellite technology', CNN, 9 February 2023, https://www.cnn.com/2023/02/09/politics/spacex-ukrainian-troops-satellite-technology/index.html.
69 Foust, J. (2023), 'Shotwell: Ukraine "weaponized" Starlink in war against Russia', SpaceNews, 8 February 2023, https://spacenews.com/shotwell-ukraine-weaponized-starlink-in-war-against-russia.
70 FitzGerald, J. (2023), 'Ukraine war: Elon Musk's SpaceX firm bars Kyiv from using Starlink tech for drone control', BBC News, 9 February 2023, https://www.bbc.co.uk/news/world-europe-64579267.

the withdrawal of support by a major private sector entity could potentially be just as damaging as a major national government leaving the coalition supporting Ukraine. The dangers of reliance on a private sector system, and the way in which lives can be saved or lost as a result of corporate decisions, were highlighted when a Ukrainian naval operation against Russian naval vessels launching missiles against Ukrainian cities was prevented from being carried out because of a personal decision by Musk not to allow the maritime drones involved to use Starlink navigation systems.[71] Musk's rationale for not enabling Starlink service to Sevastopol was that 'then SpaceX would be explicitly complicit in a major act of war and conflict escalation'.[72]

The withdrawal of support by a major private sector entity could potentially be just as damaging as a major national government leaving the coalition supporting Ukraine.

It should be noted that the Starlink example is an extreme one, both because of the Starlink network's unique prominence in Ukraine's publicly visible warfighting effort and because of its distinctive ownership and decision-making structure. But the issues it illustrates need to be addressed across the board. The balance of interests between a nation engaged in war and a corporation subject to legal and regulatory obligations, contractual obligations to customers worldwide, and obligations to a board and shareholders argues for the establishment of norms regarding clear roles, responsibilities and rules for private sector engagement in times of conflict in the distinctive operating environment created by contemporary information warfare. This would not only assist in setting expectations on both sides, but also aid corporations in their crucial decisions on whether to involve themselves in conflict, as well as informing their attitudes to possibly taking on the status of a combatant (discussed further below). At present, corporations have independently jumped in to help Ukraine, largely because they felt it was the right thing to do. The lack of any obligation to do so in future other than a moral one now suggests that governments and international organizations should do more to make it easy for those companies to decide to jump in on the right side in future conflicts too. Guidance, policy and legal cover to assist in ways that complement or supplement government action would make this decision more straightforward.

---

71 Creamer, E. (2023), 'Elon Musk biographer admits suggestion SpaceX head blocked Ukraine drone attack was wrong', *Guardian*, 12 September 2023, https://www.theguardian.com/books/2023/sep/12/elon-musk-biographer-admits-suggestion-spacex-head-blocked-ukraine-drone-attack-was-wrong.
72 Tweet by Elon Musk, 7 September 2023, https://twitter.com/elonmusk/status/1699917639043404146. Keir Giles has approached SpaceX for comment on this passage of the paper but has not received a response.

Information interdiction

In the years between 2014 and 2022, Russia devoted considerable resources to probing the vulnerabilities of civilian telecommunications infrastructure across the West, with the apparent aim of being able to disconnect this infrastructure when required and isolate target populations from outside information.[73] However, as implemented in Ukraine, with the exception of the initial Viasat attack discussed above, Russia's efforts at information interdiction were more localized and disjointed.

For Ukraine's military, the combined effect of the Viasat attack and other early information interdiction measures such as those delivered through EW has been disputed, but reporting at the tactical level suggests that Ukrainian communications were indeed suppressed, forcing reliance on civilian mobile phones.[74] This contributed to what a Ukrainian cyber official described as the later 'total domination' of the Starlink system in military communications, edging out other satellite communication systems. Meanwhile, attacks were also observed targeting Ukraine's communications infrastructure in order to reduce Ukrainian citizens' access to reliable news and information. These attacks included missile strikes on data centres[75] and television broadcasting towers, in a clear case of kinetic operations designed for information effects.[76] In late March 2022, attempts to target connectivity by cyber means achieved a severe but temporary impact on the operations of Ukrtelecom.[77] Information interdiction is one area in which Microsoft has pointed to apparently coordinated Russian cyber and kinetic attacks, as on 1 March 2022 when a missile strike against a television tower in Kyiv coincided with the launch of the DesertBlade malware attack against a broadcasting company and a statement by the Russian military that it would be targeting 'disinformation' centres. 'Attempts to compromise and or stage destructive malware on media companies is a trend that has continued throughout this conflict,' Microsoft stated.[78]

But these attacks also conflicted with a need to take over the same networks (and other infrastructure) undamaged; both sides had incentives to preserve the communications networks they were using rather than destroy them.[79] In fact,

---

73 Giles, K. and Hartmann, K. (2021), 'Adversary Targeting of Civilian Telecommunications Infrastructure', in Jančárková, T., Lindström, L., Visky, G. and Zotz, P. (eds) (2021), 13th International Conference on Cyber Conflict, https://ccdcoe.org/uploads/2021/05/CyCon_2021_Giles_Hartmann.pdf.
74 Marson, J. (2022), 'The Ragtag Army That Won the Battle of Kyiv and Saved Ukraine', *Wall Street Journal*, 20 September 2022, https://www.wsj.com/articles/russian-invasion-ukraine-battle-of-kyiv-ragtag-army-11663683336.
75 A senior strategic advisor to a major technology company, speaking under the Chatham House Rule, Tallinn, 13 May 2023.
76 Ministry of Defence (@DefenceHQ) via Twitter (2022), '(2 of 4) Russia is probably targeting Ukraine's communications infrastructure in order to reduce Ukrainian citizens' access to reliable news and information', 7 March 2022, https://twitter.com/DefenceHQ/status/1500727889192497152.
77 Peterson, A. (2022), 'Traffic at Major Ukrainian Internet Service Provider Ukrtelecom Disrupted', The Record, 28 March 2022, https://therecord.media/traffic-at-major-ukrainian-internet-service-provider-ukrtelecom-disrupted; Bing, C. and Satter, R. (2022), 'Ukrainian telecom company's internet service disrupted by 'powerful' cyberattack', Reuters, 28 March 2022, https://www.reuters.com/business/media-telecom/ukrainian-telecom-companys-internet-service-disrupted-by-powerful-cyberattack-2022-03-28.
78 Microsoft (2022), *Special Report: Ukraine: An overview of Russia's cyberattack activity in Ukraine*, 27 April 2022, https://query.prod.cms.rt.microsoft.com/cms/api/am/binary/RE4Vwwd.
79 Watling, Danylyuk and Reynolds (2023), 'Preliminary Lessons from Russia's Unconventional Operations During the Russo-Ukrainian War, February 2022–February 2023'.

the battle for access to Ukraine's mobile phone network infrastructure provides an important case study of the interdependencies between cyber, information and physical capabilities, which can sometimes give rise to conflicting priorities.

In the initial stages of the invasion, with isolated exceptions, Russian forces preserved mobile phone infrastructure largely intact – a logical outcome of the original intent to seize Ukraine rather than destroy it, despite conflicting with the aim of information interdiction.[80] But the fact that telecommunications infrastructure – including not just mobile phone sites but also internet exchange points and data centres – has largely not been subjected to systematic attack even once it became clear that it was not available for use by Russian forces has led to suspicion that Russia too exploits these facilities for access, including to government and military communications carried via encrypted channels on civilian networks. Ukrainian information practitioners point to the historical ownership by Russian business interests of telecommunications companies and subcontractors in Ukraine with access to critical data, citing this ownership as further grounds for concern that Russia's intelligence services may have mechanisms for continuing access to Ukrainian digital networks and thus the information they carry.

Ukrainian defenders chose to block all inbound roaming subscribers from Russia and Belarus, which at a stroke made them unable to communicate and also wiped out a back-up communications system for the Russian invasion forces.

Meanwhile, the start of the full-scale invasion saw thousands of new mobile phones with Russian SIM cards appearing on Ukrainian networks as the Russian soldiers carrying them – despite years of efforts by the Russian army to improve OPSEC by dissuading soldiers from indiscreet use of connected devices – moved into the country. This presented the Ukrainian defenders with their own dilemma: to block these phones and render them useless, or to allow them to continue to function so that Ukraine could intercept their communications. The choice was made to block all inbound roaming subscribers from Russia and Belarus, which at a stroke made them unable to communicate and also wiped out a back-up communications system for the Russian invasion forces. The result of this move, combined with Russia's own communications failures, was multiple instances of Russian forces stealing mobile phones from Ukrainian civilians, often with lethal force, to acquire communications capabilities and regain some degree of situational awareness.[81] This in turn facilitated Ukraine's interception of calls from Russian

80 Sabin, S. and Cerulus, L. (2022), '3 reasons Moscow isn't taking down Ukraine's cell networks', Politico, 7 March 2022, https://www.politico.com/news/2022/03/07/ukraine-phones-internet-still-work-00014487.
81 Kinetz, E. (2023), 'Over 2,000 phone calls from Russian soldiers in Ukraine intercepted', AP News, https://apnews.com/article/russia-ukraine-war-intercepts-2b14732d88b3f58d4a9d0b2b562bdb28.

forces to Russia, which were subsequently exploited including through public release of audio of Russian soldiers phoning home to openly discuss and at times boast of their participation in war crimes.[82]

Other emergency measures introduced by Ukrainian telecoms operators were designed to ensure uninterrupted connectivity for Ukraine's own citizens. These measures included blanket national roaming, so that subscribers to any Ukrainian mobile network could use the other two main providers; and a coordinated decision between operators not to suspend any account for running out of credit – as users in Russian-controlled areas, for instance, would be unable to top up their accounts with Ukrainian networks.[83]

Severe challenges in maintaining communications were reported on both sides in the earliest stages of the conflict – although just as in the invasion of Georgia 14 years earlier, on the Russian side this commonly resulted from inadequacies of equipment and planning, rather than from any action by the adversary.[84] It was widely reported that the Russian military's Era secure communications system was dependent on 3G mobile phone coverage,[85] and so when these networks were destroyed or unavailable, the system was inoperable. This reportedly led directly to losses among Russian commanders forced to communicate over insecure systems, revealing their locations and intentions.[86] If this reporting is accurate, it provides another incentive to exploit rather than destroy connectivity infrastructure. According to one assessment: '[C]yber war is deemed by the Kremlin to impede rather than enhance battlefield conditions. Attacks over the internet that are designed to damage or destroy are not nearly as attractive as maintaining access in order to collect information, shape perceptions, and gauge the effects of one's actions in other domains.'[87] In at least one instance, access by advancing Russian forces to telecommunications infrastructure was thwarted by the destruction of critical software – the digital equivalent of retreating troops blowing a bridge so that it cannot be used by the enemy.[88]

Information interdiction as apparently planned by Russia beforehand has been most easily achieved in occupied territories, where routing internet and communications access through Russia has enabled Moscow to suppress access to outside media, especially Ukrainian news platforms and essential services.[89] This has had the dual effect of enabling Russian monitoring of internet communications, through

---

82 See, for example, Krutov, M. and Yehoshyna, V. (2022), 'Russian Soldier And Wife Discussing Rape Of Ukrainian Women Identified By RFE/RL', RFE/RL, 15 April 2022, https://www.rferl.org/a/ukraine-rape-russian-soldier-wife-bykovsky/31805486.html.
83 McDaid, C. (2022), 'The Mobile Network Battlefield in Ukraine – Part 1', AdaptiveMobile Security, 29 March 2022, https://blog.adaptivemobile.com/the-mobile-network-battlefield-in-ukraine-part-1.
84 Giles, K. (2010), 'Understanding the Georgia Conflict, Two Years On – Part Two', NATO Defense College, September 2010, https://www.academia.edu/343507/Understanding_the_Georgia_Conflict_Two_Years_On_Part_Two_Vitaliy_Shlykov_Svante_Cornell_Ronald_Asmus.
85 Moss, S. (2022), 'Ukraine: Russian military's own encrypted phones impacted after destroying 3G/4G towers, allowing comms to be intercepted', Data Center Dynamics, 8 March 2022, https://www.datacenterdynamics.com/en/news/ukraine-russian-militarys-own-encrypted-phones-impacted-after-destroying-3g4g-towers-allowing-comms-to-be-intercepted.
86 GlobalData (2023), 'Unencrypted communications by Russia undermines operational security in Ukraine', Army Technology, 26 January 2023, https://www.army-technology.com/comment/unencrypted-communications-russia.
87 Kostyuk and Gartzke (2022), 'Why Cyber Dogs Have Yet to Bark Loudly in Russia's Invasion of Ukraine'.
88 Nguyen, B. (2022), 'Telecom Workers in Occupied Parts of Ukraine Destroyed Software to Avoid Russian Control over Data and Communications', Business Insider, 22 June 2022, https://www.businessinsider.com/telecom-workers-ukraine-destroyed-software-avoid-russian-control-2022-6.
89 Watling, Danylyuk and Reynolds (2023), 'Preliminary Lessons from Russia's Unconventional Operations During the Russo-Ukrainian War, February 2022–February 2023'.

the SORM system installed by default by Russian internet service providers,[90] and of leaving the population with no sources of information other than Russian propaganda.[91] Each Russian combined-arms army is supposed to have a dedicated unit tasked with 'informational isolation of the battlefield'. And documents leaked from Russia's Vulkan corporation indicated that the 'Amezit' project was designed, among other functions, to apply 'information restriction of the local area' and create an 'autonomous segment of the data transmission network' – but that this required gaining physical access to communications infrastructure.[92]

Even where Ukraine retains control of territory, Russia has achieved local success when isolated towns or communities close to the front line receive their information primarily from Russian television and radio broadcasts.[93] This has had substantial impacts on those Ukrainian populations, to be discussed further below. For other states that are potential victims of Russian aggression, the implications are clear: resilience through diversification and redundancy is critical to maintaining communications between a government and its citizens in the face of attempts at information interdiction.

Coordination

Publicly released analysis has arrived at mixed conclusions on whether Russian forces have successfully coordinated or integrated cyber effects with kinetic effects.

The head of the UK's NCSC has stated that 'Russian cyber forces from their intelligence and military branches have been busy launching a huge number of attacks in support of immediate military objectives',[94] but it is hard to identify supporting evidence from open sources. In April 2022, Microsoft concluded that 'it is unclear whether computer network operators and physical forces are just independently pursuing a common set of priorities or actively coordinating', even though 'threat activity groups often targeted the same sectors or geographic locations around the same time as kinetic military events… high concentrations of malicious network activity frequently overlapped with high-intensity fighting during the first six plus weeks of the invasion'.[95]

---

90 Soldatov, A. and Borogan, I. (2015), 'Inside the Red Web: Russia's back door onto the internet – extract', *Guardian*, 8 September 2015, https://www.theguardian.com/world/2015/sep/08/red-web-book-russia-internet.
91 Schroeder and Dack (2023), 'A parallel terrain: Public-private defense of the Ukrainian information environment'; Satariano, A. and Reinhard, S. (2022), 'How Russia Took Over Ukraine's Internet in Occupied Territories', *New York Times*, 9 August 2022, https://www.nytimes.com/interactive/2022/08/09/technology/ukraine-internet-russia-censorship.html; Bergengruen, V. (2022), 'The Battle for Control Over Ukraine's Internet', *Time*, 18 October 2022, https://time.com/6222111/ukraine-internet-russia-reclaimed-territory.
92 Harding, L. et al. (2023), '"Vulkan files" leak reveals Putin's global and domestic cyberwarfare tactics', *Guardian*, 30 March 2023, https://www.theguardian.com/technology/2023/mar/30/vulkan-files-leak-reveals-putins-global-and-domestic-cyberwarfare-tactics.
93 Gibbons-Neff, T., Yermak, N. and Hicks, T. (2022), 'Russians Breached This City, Not With Troops, but Propaganda', *New York Times*, 17 June 2022, https://www.nytimes.com/2022/06/17/world/europe/ukraine-russia-propaganda.html.
94 Chatham House (2022), 'Security and Defence Conference 2022: Speech, Lindy Cameron, CEO of the National Cyber Security Centre', 28 September 2022, https://www.ncsc.gov.uk/speech/lindy-cameron-chatham-house-security-and-defence-conference-2022.
95 Microsoft (2022), *Special Report: Ukraine: An overview of Russia's cyberattack activity in Ukraine*.

A subsequent Microsoft report in June 2022 included much more definitive language:

> On several occasions the Russian military has coupled its cyberattacks with conventional weapons aimed at the same targets. Like the combination of naval and ground forces long used in an amphibious invasion, the war in Ukraine has witnessed Russian use of cyberattacks to disable computer networks at a target before seeking to overrun it with ground troops or aerial or missile attacks.[96]

But Microsoft's references to coordination between cyber and kinetic warfare were called into question by members of the expert community,[97] and later surveys struggled to find clear examples of successful cyber–kinetic coordination.[98] Instead, there is sporadic evidence not only of lack of coordination but even, potentially, lack of communication between Russian cyber and conventional units. The UK's GCHQ points to 'red-on-red' incidents in which 'Russian military strikes took down the same networks that Russian cyber-forces were attempting to infect – ironically forcing the Ukrainians to revert to more secure means of communication'.[99]

In those limited instances where information on apparent coordination between Russian cyber and conventional units is available, it comes with caveats. It is claimed that a facility for US information warfare support for Ukraine in the Kyiv region was among the first targets for long-range precision strike missiles at the outset of the February 2022 invasion.[100] But, if true, this would be reflective of target lists drawn up long in advance rather than evidence of ongoing integrated planning. An example of coordinated action identified by cybersecurity company Mandiant, a subsidiary of Google, can be found in the attacks on the Ukraine 24 website and in a TV broadcast timed to promote and validate the contemporaneous release of a deepfake video of President Volodymyr Zelenskyy appearing to call for surrender.[101] Yet this does not provide an example of coordination across domains, since all the effects delivered were in the information space and no kinetic operation was involved, either as enabler or enabled. And even in examples like this, it is impossible to be certain that coordinated action was the intent rather than an accidental outcome. Assuming that congruence in time and location is evidence of prior planning rather than coincidence may be influenced by a common tendency to ascribe better coordination to the adversary than may be the case in real life.[102]

---

96 Microsoft (2022), *Defending Ukraine: Early Lessons from the Cyber War*, 22 June 2022, https://query.prod.cms.rt.microsoft.com/cms/api/am/binary/RE50KOK.
97 Smalley, S. (2022), 'Cybersecurity experts question Microsoft's Ukraine report', Cyberscoop, 1 July 2022, https://cyberscoop.com/cybersecurity-experts-question-microsofts-ukraine-report.
98 Bateman, J. (2022), *Russia's Wartime Cyber Operations in Ukraine: Military Impacts, Influences, and Implications*, Carnegie Endowment for International Peace, 16 December 2022, https://carnegieendowment.org/2022/12/16/russia-s-wartime-cyber-operations-in-ukraine-military-impacts-influences-and-implications-pub-88657.
99 *The Economist* (2022), 'The head of GCHQ says Vladimir Putin is losing the information war in Ukraine', 18 August 2022, https://www.economist.com/by-invitation/2022/08/18/the-head-of-gchq-says-vladimir-putin-is-losing-the-information-war-in-ukraine.
100 Howe, E. (2022), 'Army Special Ops Is Changing Psyops Training to Reflect Ukraine War', Defense One, 8 November 2022, https://www.defenseone.com/threats/2022/11/army-special-ops-changing-psyops-training-reflect-ukraine-war/379500.
101 Google Threat Analysis Group (2023), 'Fog of war: how the Ukraine conflict transformed the cyber threat landscape'.
102 Wilde, G. (2022), 'Assess Russia's Cyber Performance Without Repeating Its Past Mistakes', War on the Rocks, 21 July 2022, https://warontherocks.com/2022/07/assess-russias-cyber-performance-without-repeating-its-past-mistakes.

Similarly, there has been sporadic reporting of Russian cyber forces trying to use captured Ukrainian military information technology such as tablets to gain access to Ukrainian networks; but without knowledge of how this access was to have been exploited, it is not possible to tell whether this should be considered an espionage campaign, an attempt to facilitate conventional operations, neither, or both.[103]

Russia's integration of cyber effects into its military campaign appears to have evolved in parallel with the distinct phases of the war itself.

Gavin Wilde, an expert on Russian information warfare, suggests that an apparent paucity of evident integration with kinetic operations may result from the operating ethos of Russia's cyber forces, since 'Russia's premier offensive cyber capacities are housed within agencies focused on intelligence and subversion – the key tool kits used against Ukraine since 2014 – rather than combined-arms warfare'. Consequently, Wilde continues, 'even the most brazen and destructive cyberattacks historically unleashed in Ukraine appear to be part of a sociopolitical pressure campaign, not particularly intended to achieve any discrete, time-bound, or geographic objectives'.[104] While this observation relates primarily to the period before 2022 and the arrival of full-scale open conflict, even with the caveat that there is little public knowledge of incidents targeting Ukraine's military it is notable that the majority of observed Russian cyber activity since that point still represents 'countervalue', rather than 'counterforce', targeting. This includes attempts at exploitation of successful (or even unsuccessful) cyber operations to demoralize the Ukrainian civilian population.[105] This in turn indicates how, in keeping with Russia's holistic concept of information operations, 'Cyber operations are a form of modern political warfare, rather than decisive battles. These operations don't win wars, but instead support espionage, deception, subversion and propaganda efforts.'[106]

This highlights the limitations of considering Russian cyber fires as a direct alternative, or substitute, for kinetic activities to achieve a given effect. Cyber operations instead provide a supplementary capability with a different range of effects to the physical destruction of the target. Accordingly, Russia's integration of cyber effects into its military campaign appears to have evolved in parallel with the distinct phases of the war itself. The initial wave of attacks before and during the February 2022 invasion aimed to produce disruptions to shape the battlespace and create a more permissive environment for the follow-on conventional activities. As the war developed, access operations to gain situational awareness became more prominent, targeting Ukrainian military applications such as Delta and Bachu, or webcams and CCTV services both in the area of operations and on Ukraine's western border to try to identify the delivery of Western aid. The Russian

---

103 Antoniuk (2023), 'Ukraine says it thwarted attempt to breach military tablets'.
104 Wilde (2022), *Cyber Operations in Ukraine: Russia's Unmet Expectations*.
105 Black, D. (2023), 'Russia's War in Ukraine: Examining the Success of Ukrainian Cyber Defences', International Institute for Strategic Studies (IISS), https://www.iiss.org/research-paper/2023/03/russias-war-in-ukraine-examining-the-success-of-ukrainian-cyber-defences.
106 Lonergan, E. D., Lonergan, S. W., Valeriano, B. and Jensen, B. (2022), 'Putin's invasion of Ukraine didn't rely on cyberwarfare. Here's why', *Washington Post*, 7 March 2022, https://www.washingtonpost.com/politics/2022/03/07/putins-invasion-ukraine-didnt-rely-cyber-warfare-heres-why.

campaign against Ukrainian energy infrastructure in the autumn of 2022 indicated operational-level coordination of different disruptive cyber capabilities with kinetic strikes to maximize both physical and psychological impact. This evolution points to an agility and adaptability on the part of Russia's cyber forces that in turn suggest further increases in sophistication are likely as the war continues.

Overall, combined cyber and kinetic operations have been far less visible than might be assumed by Western audiences, especially if there is an assumption of cyber power being exercised primarily for kinetic or physical effect. As the war has moved on, the potential physical impacts of cyber operations have faded still further in relative significance. Wiper malware attack campaigns were noted against a wide range of targets both before and after February 2022,[107] but during Russia's campaign overall, any physical impact achieved through cyber means was entirely overshadowed by the direct effects of missile and drone strikes.[108] In part, this is a simple function of the asymmetry of investment required in delivering destructive effects through cyber or kinetic means. One analysis makes the following argument about like-for-like comparisons:

> [E]ven the most sophisticated offensive cyber operations can't compete with conventional munitions. It's far easier to target the enemy with artillery, mortars and bombers than with exquisite and ephemeral cyber power. Notwithstanding any cyber vulnerabilities, it's much simpler for Russia to launch an artillery barrage at a power substation than to hack it from Moscow.[109]

Cyber effects beyond the theatre

Another unfulfilled expectation was that there would be widespread international spillover from cyber operations against Ukraine, with uncontained cyber weapons causing significant damage either deliberately against the West or accidentally against the world.[110] Yet despite an intensive Russian campaign against overseas Ukrainian diplomatic missions, which on occasion presented softer targets than the Ministry of Foreign Affairs in Kyiv, the expected direct and intentional impacts on the US and other Western countries did not materialize in the early stages of the escalation.[111] The pace and intensity of publicly reported Russian and Russian-backed cyber campaigns against Western targets appear to have remained largely comparable with the period before 2022,[112] and Google 'didn't observe a surge of attacks against critical infrastructure outside… Ukraine'.[113]

---

107 Raffray, E. (2022), 'Ukraine: 100 days of war in cyberspace', Cyber Peace Institute, 2 June 2022, https://cyberpeaceinstitute.org/news/Ukraine-100-days-of-war-in-cyberspace.
108 Astier, H. and Lukov, Y. (2022), 'Ukraine war: Massive Russian strikes target energy grid – Zelensky', BBC News, 23 October 2022, https://www.bbc.co.uk/news/world-europe-63357393.
109 Lonergan, Lonergan, Valeriano and Jensen (2022), 'Putin's invasion of Ukraine didn't rely on cyberwarfare. Here's why'.
110 Willett, M. (2022), 'Russia–Ukraine: Pressing the right button at the right time', IISS, 10 March 2022, https://www.iiss.org/online-analysis/online-analysis/2022/03/russia-ukraine-pressing-the-right-button-at-the-right-time.
111 Demarest, C. (2022), 'US seeking to understand Russia's failure to project cyber power in Ukraine', C4ISRNET, 21 July 2022, https://www.c4isrnet.com/cyber/2022/07/21/us-seeking-to-understand-russian-failures-to-project-cyber-power-in-ukraine.
112 Center for Strategic & International Studies (CSIS) (undated), 'Significant Cyber Incidents', https://www.csis.org/programs/strategic-technologies-program/significant-cyber-incidents.
113 Google Threat Analysis Group (2023), 'Fog of war: how the Ukraine conflict transformed the cyber threat landscape'.

The period of intensified fighting in Ukraine has coincided with a rise in frequency and impact of cyber incidents globally, but analysis by SecDev, a digital resilience foundation, attributes this more to the rapidity of digital transformation than to interstate competition.[114] According to Ciaran Martin, the former head of the UK's NCSC, speaking in November 2022: 'Despite all the hype, Putin has not seriously troubled the West at all in cyberspace since the invasion.'[115] Another, unnamed, British official concludes that Russia was keen to confine the impact of its attacks to Ukraine in order to avoid a confrontation with NATO nations.[116]

The cyber incident that caused the most widely reported collateral damage outside Ukraine itself was the Viasat attack at the outset of the new invasion, which resulted in a partial interruption of KA-SAT's satellite broadband service. The attack affected not only tens of thousands of broadband customers across Europe, but also the operations of 5,800 wind turbines in central Europe.[117] More recently, Russia has shown itself willing to carry out cyber, but not kinetic, attacks on the logistics chains and organizations delivering aid to Ukraine through Poland.[118] Notably, one attack on Poland used Prestige ransomware, providing a degree of deniability and disguise as criminal activity now seen less frequently in attacks within Ukraine itself.[119] The same efforts to avoid detection were evident in Russia's covert campaign to instigate sabotage of Poland's rail network.[120] This could indicate that Russia's understanding of NATO's Article 5 agreement on collective defence is shaping the boundaries of Russian actions[121] – and that cyber activity is still considered less escalatory than direct kinetic attack.

This interpretation will have been confirmed, in Russian eyes, by Western reactions to the Viasat hack and the collateral damage it caused. Western governments confined themselves to 'condemning the attack in the strongest possible terms' – in other words, just as with warlike acts directed against Europe in the period 2014–22, they did not respond in any manner that would be meaningful to Moscow. This implies that if Russia wishes to escalate the conflict further as part of its deterrent strategy, direct and more damaging cyberattacks against Western interests would provide a more attractive option than the nuclear strike option that is far more prominent in Western public discussion.

Meanwhile, Russian cyber operations directed further afield since 2022 have received relatively scant publicity. In February 2023, a joint report by the Netherlands' intelligence and security services listed a wide range of both cyber

---

114 SecDev (2022), 'Europe's Digital Troubles', October 2022, https://mailchi.mp/secdev/europes-digital-troubles.
115 *The Economist* (2022), 'Lessons from Russia's cyber-war in Ukraine'.
116 Ibid.
117 Reuters (2022), 'Satellite outage knocks out thousands of Enercon's wind turbines', 28 February 2022, https://www.reuters.com/business/energy/satellite-outage-knocks-out-control-enercon-wind-turbines-2022-02-28.
118 Lyngaas, S. (2023), 'Russian hackers targeted European military and transport organizations in newly discovered spying campaign', CNN, 15 March 2023, https://edition.cnn.com/2023/03/15/politics/russian-hackers-europe-military-organizations-microsoft/index.html.
119 Greig, J. (2022), 'Microsoft attributes 'Prestige' ransomware attacks on Ukraine and Poland to Russian group', *The Record*, 10 November 2022, https://therecord.media/microsoft-attributes-prestige-ransomware-attacks-on-ukraine-and-poland-to-russian-group.
120 Miller, G. (2023), 'Russia recruited operatives online to target weapons crossing Poland', *Washington Post*, 16 August 2023, https://www.washingtonpost.com/world/2023/08/18/ukraine-weapons-sabotage-gru-poland.
121 Kaminska, M., Shires, J. and Smeets, M. (2022), *Cyber Operations during the 2022 Russian invasion of Ukraine: Lessons Learned (so far)*, European Cyber Conflict Research Initiative, https://eccri.eu/wp-content/uploads/2022/07/ECCRI_WorkshopReport_Version-Online.pdf.

and physical 'espionage and preparatory acts for disruption and sabotage'[122] – but this was an exception. In a distinctive break from the apparent pattern of openness and transparency that briefly marked the preceding period,[123] Western security and intelligence agencies have relapsed into their previous habit of secrecy around specific threats to the societies they protect.

Reporting on successful offensive cyber operations by Ukraine is isolated, patchy and insufficient for forming overall conclusions as to the nature of the campaign Ukraine might be waging.

Similarly, limited information is available in the public domain to assess the success or impact of Russian cyberattacks against Ukrainian government or military forces, or indeed those of Ukraine against Russia. This is because Ukraine's habitual reticence regarding cyber operations it has carried out against Russia is mirrored by a successful policy of not disclosing the impact of attacks against itself. The result is that reporting on successful offensive cyber operations by Ukraine is isolated, patchy and insufficient for forming overall conclusions as to the nature of the campaign Ukraine might be waging.

Incidents that have been attributed to Ukrainian cyber action include destructive attacks on Russia's oil and gas infrastructure,[124] sometimes allegedly repeated due to Russian inability to address vulnerabilities. One report quotes an alleged Ukrainian government cyber operative as commenting: 'Same pipeline. Same exploit. Everything same as before. They did nothing at all to their security. Those *&@#* never learn.'[125] Russian defence industry installations have allegedly also been targeted by Ukraine.[126] Operations may include false flag attacks designed to exploit internal divisions within Russia. One apparent example may have been an incident disrupting Russian military satellite communications, which in one account was attributed to a group aligned with the Wagner private military company in the wake of its abortive mutiny in June 2023.[127]

Effects are delivered not only by Ukrainian state agencies, but also by civilians acting independently. According to one assessment, these individuals may choose from a wider target set than 'official' cyber forces. They may engage in vandalism to impose costs on the Russian economy – such as by targeting railway systems or the

---

122 Martin, A. (2023), 'Dutch intelligence: Many cyberattacks by Russia are not yet public knowledge', The Record, 22 February 2023, https://therecord.media/dutch-intelligence-russia-cyberattacks-many-not-yet-public-knowledge.
123 Giles, K. and Hartmann, K. (2019), '"Silent Battle" Goes Loud: Entering a New Era of State-Avowed Cyber Conflict', 2019 11th International Conference on Cyber Conflict, CCDCOE, June 2019, https://ccdcoe.org/uploads/2019/06/Art_02_Silent-battle-Goes-Loud.pdf.
124 Cole, B. (2023), 'Explosion Rocks Gas Pipeline in Russia', *Newsweek*, 30 March 2023, https://www.newsweek.com/russia-blast-gas-gazprom-rocks-1791425.
125 Caruso, J. (2023), 'Another Gazprom Pipeline Explosion', Inside Cyber Warfare, 2 April 2023, https://www.insidecyberwarfare.com/p/another-gazprom-pipeline-explosion.
126 Bezpalko, U. and Kucheryavets, M. (2023), 'ГУР провело масштабную кибератаку на оборонный завод' [GUR carries out major cyberattack on defence factory], RBK Ukraina, 30 March 2023, https://www.rbc.ua/ukr/news/gur-provelo-masshtabnu-kiberataku-oboronniy-1685433575.html.
127 Menn, J. (2023), 'Cyberattack knocks out satellite communications for Russian military', *Washington Post*, 30 June 2023, https://www.washingtonpost.com/technology/2023/06/30/satellite-hacked-russian-military.

national food quality authentication system, or facilitating information operations by enabling broadcast of pro-Ukrainian messaging across Russian television and radio networks.[128] This latter campaign has reportedly had a severe impact on domestic television channels broadcasting within Russia,[129] with jamming or hacking becoming so effective that at one point the national transmitter operator, RTRS, sought to protect the main domestic channels by rebroadcasting their programming via a military satellite.[130]

Legality and legitimacy

One of the fundamental distinctions between the parties to the conflict is that Ukraine is a democracy governed by the rule of law, while Russia has no such constraints. This has obliged Ukraine to adapt its legislative framework for information and cyber activities rapidly under the pressure of war.

For many countries, the demonstrated need for data evacuation ahead of a conventional conflict may clash with peacetime data security requirements that might specify that government data must be held on sovereign territory. In the case of Ukraine, this challenge was addressed by rapid amendments to data protection law, enacted by Ukraine's parliament as late as 17 February 2022. Other legal initiatives have included attempts to regulate and regularize the status of Ukraine's 'IT Army' of volunteer cyber activists,[131] and the adoption of special legal measures authorizing remote access by Microsoft to computers across the country (this access was needed to turn on controlled folder access in Microsoft Defender security systems in order to mitigate the impact of Russian malware attacks).[132] The rapid passage of legislation demonstrates an administrative agility and degree of national consensus that might be hard to achieve in other states. On a more academic and theoretical level, it also raises the question of what precisely constitutes adherence to the rule of law when the law itself can be so deftly adjusted to suit current circumstances.

Other legal considerations arise from the nature of the conflict as a war of national survival calling on all citizens to be involved in defence – specifically, from concerns over the erosion of the distinction between combatants and civilians.[133]

---

128 Tidy, J. (2023), 'Meet the hacker armies on Ukraine's cyber front line', BBC News, 15 April 2023, https://www.bbc.co.uk/news/technology-65250356.
129 Notchenko, V. (2023), 'Россияне почти месяц живут без нормального телевидения' [Russians have been living without normal television for almost a month], GlavSovet, 7 July 2023, https://sovetov.su/news/2023/7/7/35395.
130 Greenway, C. (@ChrisGreenwayUK) via Twitter (2023), 'Ukraine's jamming/hacking of Russian TV has become so effective that Russia's national transmitter operator RTRS has put the main domestic channels on a *military* satellite, perhaps hoping that will be harder to jam. (Satellite is Cosmos 2520 at 45 East.)', 15 June 2023, https://twitter.com/chrisgreenwayuk/status/1669314208947732486.
131 Waterman, S. (2023), 'Ukraine Scrambles to Draft Cyber Law, Legalizing Its Volunteer Hacker Army', *Newsweek*, 14 March 2023, https://www.newsweek.com/ukraine-drafting-new-law-legalizing-volunteer-hacker-cyber-army-red-cross-1786814.
132 Microsoft (2022), *Defending Ukraine: Early Lessons from the Cyber War*.
133 Mačák, K. (2023), 'Will the centre hold? Countering the erosion of the principle of distinction on the digital battlefield', *International Review of the Red Cross*, 10 May 2023, pp. 1–27, https://doi.org/10.1017/S1816383123000152.

The involvement of private citizens in cyber and information activities mirrors the efforts of other volunteer groups supporting all aspects of Ukraine's war effort.[134] Ukraine's 'Diia' civilian government services app incorporates an 'e-Enemy' function to allow private citizens to report Russian troop locations and movements. Information from this function feeds into 'Delta', the Ukrainian military's situational awareness platform.[135] Thus civilians are encouraged to engage in combat support activities. The collection of open-source information also aids in establishing accountability for war crimes and atrocities.[136] This, too, could be considered an operational impact – at least, Russia has indicated so through its previous actions targeting organizations such as the World Anti-Doping Agency and the Organisation for the Prohibition of Chemical Weapons because they held evidence that promised reputational damage for Russia.[137] In Ukraine, being detected by Russian forces in the occupied territories or near the front line as having reported troop movements or holding compromising evidence of this kind invites inevitable swift, vicious and potentially fatal consequences. This is a particular hazard if apps route sensitive communications over messaging services such as Telegram. Ukrainian citizens who have returned from Russian captivity have reported that their FSB interrogators had copies of their Telegram messages, even though the former prisoners believed these to have been securely deleted months previously – one of many possible explanations being that the messages were intercepted through Russia's SORM system described above.

There is a strong legal argument that smartphone users reporting military movements forfeit their protected status as civilians.[138] This principle is said to have been applied, for example, by Western forces in theatres such as Afghanistan, where individuals engaging in this activity could be treated as enemy combatants.[139] In the case of Russia's war on Ukraine, the point is largely academic, since Russia does not observe principles of international humanitarian law (IHL) so the protections this provides are moot in practical terms. However, the widespread engagement of civilians in direct support of hostilities could potentially undermine their entitlement to protection in the view of the international community too. According to one analysis, such engagement implies not only that Ukrainian civilians can be lawfully killed or injured by Russian troops without any corresponding legal right to fight back, but also that, if detained, they have none of the notional protections

---

134 Guest, P. (2023), 'Ukraine War: How to Win With Trucks, Trolls, and Tourniquets', WIRED, 6 July 2023, https://www.wired.com/story/ukraine-war-trucks-trolls-tourniquets.
135 Danylov, O. (2023), 'The unique Ukrainian situational awareness system Delta was presented at the annual NATO event', Mezha, 28 October 2022, https://mezha.media/en/2022/10/28/the-unique-ukrainian-situational-awareness-system-delta-was-presented-at-the-annual-nato-event.
136 Pomerantsev, P. (2023), 'Letter from Ukraine', *The Spectator*, 8 March 2023, https://app.spectator.co.uk/2023/03/08/letter-from-ukraine-3/content.html.
137 See Sanders-Zakre, A. (2018), 'Russia Charged With OPCW Hacking Attempt', Arms Control Association, November 2018, https://www.armscontrol.org/act/2018-11/news/russia-charged-opcw-hacking-attempt; CNBC (2018), 'Dutch government says it disrupted Russian attempt to hack chemical weapons watchdog', 4 October 2018, https://www.cnbc.com/2018/10/04/dutch-government-disrupted-russian-attempt-to-hack-chemical-weapons-watchdog.html; Harding, L. (2018), 'How Russian spies bungled cyber-attack on weapons watchdog', *Guardian*, 4 October 2018, https://www.theguardian.com/world/2018/oct/04/how-russian-spies-bungled-cyber-attack-on-weapons-watchdog; UK Foreign & Commonwealth Office (2018), 'Minister for Europe statement: attempted hacking of the OPCW by Russian military intelligence', 4 October 2018, https://www.gov.uk/government/speeches/minister-for-europe-statement-attempted-hacking-of-the-opcw-by-russian-military-intelligence.
138 Olejnik, L. (2022), 'Smartphones Blur the Line Between Civilian and Combatant', WIRED, 6 June 2022, https://www.wired.com/story/smartphones-ukraine-civilian-combatant.
139 Chatham House (2023), 'The use of Open-Source Intelligence (OSINT) in Ukraine: lifting the fog of war or blurring it further?', closed discussion, Chatham House, 21 March 2023.

of prisoners of war. Furthermore, according to one analysis, 'widespread civilian participation in the targeting process can make it more difficult to prove Russian breaches of IHL and thus make it more difficult to prosecute members of the Russian armed forces for the war crime of intentionally directing attacks against civilians'.[140]

The Delta system further potentially blurs the legal status of commercial entities. In February 2023 Ukraine announced plans to host the system on cloud servers outside Ukraine,[141] for the same rationale of resilience that led government data to be evacuated from Ukraine and hosted by Amazon. Whose servers precisely were intended to host Delta remained, understandably, unspecified; but if a military system facilitating active combat operations is hosted on a civilian cloud service, there seems little doubt that Russia would consider that civilian commercial entity a valuable target for direct action of some sort designed to compromise or deter its operations.

Thus, while the risk to individuals within Ukraine is immediate, there is a further issue regarding the practical risk that civilian enablers of Ukrainian offensive or defensive operations further afield may be exposed to – for example, the staff of foreign cybersecurity and technology companies providing services and assistance to Ukraine.[142] That risk is not, as yet, known to have been borne out by attacks on these civilian personnel by Russia, but Russia has shown itself able and eager to reach into Western countries to target individuals through active measures,[143] so this remains a distinct possibility in the future, and one for which Western commercial entities should be fully prepared.

Conversely, there is also a strong argument that Russian cyberattacks on civilian infrastructure could be prosecuted as war crimes.[144] However, this notion faces the same challenges as enforcement of accountability for Russia overall – up to and including the International Criminal Court warrant issued for President Vladimir Putin himself – so remains in the realm of theory and may not present any practical deterrent to continued illegal actions. The speed of events in open conflict is also prejudicial to investigation and accountability: the need for instant remediation of cyber incidents to keep systems running has at times to be prioritized over the long and labour-intensive process of collection and preservation of evidence for intelligence, prosecution or deep analysis use. Just as standalone cyber operations have the luxury of time for their developers to design, perfect and deploy them, while tactical cyber operations in wartime often do not, so defenders will often not have the time or resources to invest in the data collection required for subsequent detailed analysis of attacks for forensic or intelligence purposes.

---

140 Winther, P. and Nilsson, P.-E. (2023), *Smart Tactics or Risky Behaviour? The Lawfulness of Encouraging Civilians to Participate in Targeting in an Age of Digital Warfare*, Hague Centre for Strategic Studies, May 2023, https://hcss.nl/wp-content/uploads/2023/05/02-Smart-Tactics-or-Risky-Behaviour.pdf.
141 Ministry of Defence of Ukraine (2023), 'Government approves decision to introduce Delta system in the Defense Forces', 4 February 2023, https://www.kmu.gov.ua/en/news/uriad-ukhvalyv-rishennia-shchodo-zaprovadzhennia-systemy-delta-v-sylakh-oborony.
142 Zetter, K. (2022), 'Security Firms Aiding Ukraine During War Could Be Considered Participants in Conflict', Zero Day, 7 December 2022, https://zetter.substack.com/p/security-firms-aiding-ukraine-during.
143 As described in detail in Giles, K. (2022), *Russia's War on Everybody: And What it Means for You*, London: Bloomsbury.
144 Freeman, L. (2022), 'Russian Cyberattacks Need an International Criminal Court Response', Center for European Policy Analysis (CEPA), 19 July 2022, https://cepa.org/article/russian-cyberattacks-need-an-international-criminal-court-response.

Personalized identification of individuals for attack is in part a function of the huge expansion of potential targets available for exploitation, including personal phones and connected devices.[145] The early stages of the war exposed the critical – and in fact lethal – nature of personal data in general. Russia had directed focused efforts at gaining access to public and private databases, including not only government information such as tax and residence records but also medical records and commercial data like details of insurance accounts. This information was then used to identify individuals to be detained, imprisoned or murdered in the occupied territories, with those with prior military service at particular risk.[146] Meanwhile, an initial lack of awareness of these dangers meant that large amounts of personal information were being insecurely collected in the context of large population movements across the country and beyond it. Urgency led to the recording of personal information, identity documents and relationships in insecure spreadsheets at locations near Ukraine's borders, which were then translated and/or transmitted using insecure systems and apps, all presenting a soft target for exploitation by hostile actors. The weaponization of information as apparently innocuous as health records provides another vital lesson for countries that may at some future point find themselves under attack by Russia or any other state that may be inclined to adopt similar methods.

145 Satter, R. (2022), 'Ukrainian officials' phones targeted by hackers – cyber watchdog', Reuters, 6 June 2022, https://www.reuters.com/world/europe/ukrainian-officials-phones-targeted-by-hackers-cyber-watchdog-2022-06-06.
146 Watling, Danylyuk and Reynolds (2023), 'Preliminary Lessons from Russia's Unconventional Operations During the Russo-Ukrainian War, February 2022–February 2023'.

04 Information confrontation: human effects

Disinformation and influence campaigns are an integral part of Russia's concept of information warfare. The failure of these campaigns' strategic objectives in Ukraine has ensured that country's survival; but Russia has been successful both directly against Western countries and elsewhere around the world.

Information effects within Ukraine

Within Ukraine itself, Russia's attempts to influence both military personnel and civilians have been intensive and widespread but have shown little evidence of substantial strategic impact since February 2022. This, too, is a result of the extensive prior duration of the conflict; Ukrainian targets of disinformation operations have long been accustomed to the methods in play.[147] In the face of ongoing information warfare from Russia, Ukraine launched multiple initiatives aimed at improving coordination and building resilience between 2015 and 2021, in some cases sponsored and facilitated by foreign governments, including the UK. As a result, Ukrainians were relatively well prepared in this domain when Russia launched its full-scale invasion in February 2022.[148]

147 Erlich, A. and Garner, C. (2023), 'Is pro-Kremlin Disinformation Effective? Evidence from Ukraine', *The International Journal of Press/Politics*, 2023, Vol. 28(1) 5–28, DOI: 10.1177/19401612211045221.
148 FOI (2023), 'War of words – how Ukraine uses strategic communication to beat Russia on the information front', 21 April 2023, https://www.foi.se/en/foi/news-and-pressroom/news/2023-04-21-war-of-words---how-ukraine-uses-strategic-communication-to-beat-russia-on-the-information-front.html.

If Russia had succeeded in dividing or demoralizing the Ukrainian population, or eroding its faith in and support for institutions in the manner that other Russian campaigns against the West have sought to do, this could have had a critical impact on the essential resilience and unity that has enabled Ukraine to prevail to date. However, the fundamental failure of Russia's intelligence agencies and planners to grasp that Ukraine was a separate country that would resist a Russian attack meant that efforts in this direction were misguided, misconceived and insufficient. Campaigns of subversion targeting Ukraine's population and decision-makers achieved far less effect than was optimistically reported to the Kremlin.[149]

The result was a catastrophic misjudgment of the probable response of Ukrainians to the invasion and an expectation that military activity could be limited to decapitation strikes, followed by the arrest of a limited number of Ukrainian patriots, after which even a low level of active collaboration would ensure control by Russian forces over the remainder of the population.[150] The outcome of this misjudgment has been both beneficial and tragic for Ukraine. It doomed Russia's operational plan to failure, but it also was a key reason for the launch of the invasion in the first place, and then for its rapid transition into a campaign with genocidal aims once it became clear that Ukrainians were failing to conform to Russia's misguided caricature of them as frustrated and slightly inferior Russians yearning for liberation.

This does not mean that Russia has not achieved local information successes. Russia's ability to find and exploit collaborators was a key enabler for its success in occupying some southern regions of Ukraine with very little opposition. Embedded Russian agents also engaged in technical information warfare, such as SMS broadcasting and communications interception, deep within Ukrainian territory.[151] Within Ukrainian government-held territory, individuals acting in support of Russia have repeatedly been detained for providing targeting information to Russian forces. Preparations for the invasion included renting private apartments to use as bases for electronic surveillance of individuals in the local area, including interception of their communications and activity on social networks – an important element in building Russia's awareness of whom to target for elimination after the invasion. Other facilities established by Russia deep within Ukraine included rebroadcasting stations distributing disinformation via SMS directly on to cellphone networks.[152]

Long-standing propaganda and disinformation efforts aimed at the civilian inhabitants of occupied areas of the east of the country have had a cumulative effect, leading to cognitive dissonance when those areas are liberated by Ukrainian forces – a problem that will pose a significant challenge if or when Crimea too is recovered from Russian occupation. Pro-Russian sentiment can be strong among populations within reach of broadcast media from occupied areas, even in the face

---

149 Foy, H. and Rathbone, J.P. (2022), 'Intelligence failures hamper Russia's Ukraine mission', *Financial Times*, 1 March 2022, https://www.ft.com/content/ba440d90-b0ba-4a73-a138-9cb1229b6cac.
150 Watling, Danylyuk and Reynolds (2023), 'Preliminary Lessons from Russia's Unconventional Operations During the Russo-Ukrainian War, February 2022–February 2023'.
151 Faife, C. (2022), 'A phone relay capture may be the latest of Russia's communications woes in Ukraine', The Verge, 15 March 2022, https://www.theverge.com/2022/3/15/22979381/phone-relay-capture-russia-military-unencrypted-communications-ukraine.
152 McDaid, C. (2022), 'The Mobile Network Battlefield in Ukraine – Part 1', AdaptiveMobile Security, 29 March 2022, https://blog.adaptivemobile.com/the-mobile-network-battlefield-in-ukraine-part-1.

of the reality of the war, aided by highly localized Russian information campaigns via Telegram channels, which can 'announce that the Ukrainian Army is firing mortars just before a Russian missile strike hits'.[153]

Cyberattacks, when not tied to an immediate tactical or operational aim, have appeared designed to contribute to intimidating and demoralizing the Ukrainian defenders: '[E]ven if an attack's immediate effect can be qualified as destructive – be it data wiping, denial of service, or even causing a short-term blackout – the actual goal for these operations appears to be cognitive in its nature: the (often limited) value lies in sending a certain message or causing distress and confusion.'[154] But the overall impact appears limited – once again, cyber effects lose relative significance in the context of open warfare. In addition, Ukrainian OPSEC has helped to deny the intended cognitive outcomes, or desired secondary effects, of Russian cyberattacks. When Russia wants to mount an information campaign exploiting the impact of successful cyber operations to demoralize Ukrainians, this intent is frustrated if that effect is not made public.[155] This supports the conclusion that OPSEC is vital not only in a military context, but also through the whole of society when it faces a holistic information exploitation threat.

Ukrainian strategic communications have been a whole-of-society effort, in cooperation between the government, military, news media and civil society.

In fact, Ukrainian defensive preparations have proved effective across the board. This has included the banning of Russian media and journalists ahead of the invasion, a move judged relatively controversial at the time, but subsequently found to be justifiable given their role in 'threatening the continued development of democracy in Ukraine: via eroding public support for democracy; via distorting perceptions of truth and thereby hindering rational debate and via weakening the morale needed to fuel resistance and defence of the democratic state in the case of physical attack'.[156] Meanwhile, Ukrainian strategic communications have been a whole-of-society effort, in cooperation between the government, military, news media and civil society. This effort has been greatly facilitated by the predominance of skilled communicators in senior positions in the Ukrainian government, enabling agile, proactive and engaging strategic communications making full use of modern media tools, in stark contrast with Russian – and sometimes Western – efforts.[157]

---

153 Gall, C., Chubko, O. and Shapoval, D. (2023), 'How Russian Propaganda Plagues Parts of Eastern Ukraine', *New York Times*, 19 April 2023, https://www.nytimes.com/2023/04/19/world/europe/ukraine-russia-donbas-propaganda.html.
154 Rõigas, H. (2022), 'Bits versus Bombs: Observations on Russian Offensive Cyber Operations in Ukraine', International Centre for Defence and Security (ICDS), 13 December 2022, https://icds.ee/en/bits-versus-bombs-observations-on-russian-offensive-cyber-operations-in-ukraine.
155 Black (2023), 'Russia's War in Ukraine: Examining the Success of Ukrainian Cyber Defences'.
156 Szostek, J. and Orlova, D. (2023), 'Free speech versus defence of the nation? The media as sources of national insecurity in Ukraine', *European Security*, 13 July 2023, https://www.tandfonline.com/doi/full/10.1080/09662839.2023.2231369.
157 FOI (2023), 'War of words – how Ukraine uses strategic communication to beat Russia on the information front'.

Russian tactical information operations directed at Ukrainian military personnel in a particular local area include means of disseminating information that remain unchanged from conflicts in the previous century – and are therefore completely independent of the internet. These include radio broadcasts,[158] the use of long-range loudspeakers,[159] and leaflet distribution by artillery shell.[160] Meanwhile, direct messages to Ukrainian military personnel containing personalized threats – for instance, including information on their families and residences as well as their names – are delivered by SMS, Telegram, Viber, Signal and WhatsApp.[161] However, this is a technique that has been noted since the very earliest stages of the conflict in 2014–15, allowing ample time for it to become an accepted feature of the information environment, which in turn is likely to limit its effectiveness.[162] Reporting on messaging of this kind in mid-2022 noted that despite evidence of some agility in messaging, such as threatening the defenders of Sievierodonetsk that they faced 'another Mariupol',[163] the majority of personal information used was outdated.[164] In some cases, Russia's misconceptualization of the conflict as a whole has also undermined its information campaigns – during the siege of the Azovstal steelworks in Mariupol, Russian propaganda directed at the Ukrainian defenders through the internet, radio, loudspeakers and leaflet drops leaned heavily on the narrative that 'Kyiv is unable to control the nationalists in the armed forces', an approach which unsurprisingly was found to be ineffective.[165]

An apparent inability to keep pace with the evolution of the information environment casts doubt on Russia's future ability to exploit rapidly developing fully synthetic media, long described as another potential game-changer in disinformation and deception operations.[166] The release in mid-March 2022 of a deepfake video of President Zelenskyy purportedly calling on Ukrainians to surrender provides an illustration of Russia being behind the curve both technically and conceptually. The deepfake was of low quality and would have been unconvincing even if it had been released several years earlier when deepfakes themselves were a novelty. Its use in this instance was both several weeks out of date – in the sense that it would have been far more effective at the outset of the invasion – and several years out of date, in the sense that target audiences were already familiar with the concept of deepfakes, since they had been so widely used and discussed in preceding years.[167]

---

158 Gibbons-Neff, Yermak and Hicks (2022), 'Russians Breached This City, Not With Troops, but Propaganda'.
159 Juurvee, I. via YouTube (2023), 'Russian Tactical PSYOPS in Ukraine – do they play by Soviet handbook?', presentation at 'Russia's war on Ukraine: strategic and operational designs and implementation', video, 6 February 2023, https://www.youtube.com/watch?v=iI-1U5kKwd8.
160 Lavrov, A. and Pukhov, R. (eds) (2022), 'Война среди стен' [War Within Walls], CAST, Moscow, 2022.
161 Main Directorate of Intelligence of the Ministry of Defence of Ukraine (2022), 'Увага! Ворог розсилає погрози. Не піддавайтесь на провокації!' [WARNING! The enemy sends threats. Do not give in to provocations!], 8 June 2022, https://gur.gov.ua/content/uvaha-voroh-rozsylaie-pohrozy-ne-piddavaites-na-provokatsii.html.
162 Giles (2015), 'The Next Phase of Russian Information Warfare'.
163 Lemekha, S. (2022), 'Сєвєродонецьк стане другим Маріуполем – експерт про нову іпсошну операцію росіян' [Sievierodonetsk will become a second Mariupol, says an expert on the Russians' new psyops operation], ArmiyaInform, 8 June 2022, https://armyinform.com.ua/2022/06/08/syevyerodoneczk-stane-drugym-mariupolem-tysyachi-ukrayinskyh-voyiniv-zdadutsya-v-polon-ekspert-pro-novu-ipsoshnu-operacziyu-rosiya.
164 Main Directorate of Intelligence of the Ministry of Defence of Ukraine (2022), 'Увага! Ворог розсилає погрози. Не піддавайтесь на провокації!' [WARNING! The enemy sends threats. Do not give in to provocations!].
165 Lavrov and Pukhov (eds) (2022), 'Война среди стен' [War Within Walls], pp. 129–30.
166 Thompson, H. D. (2022), 'Worse than 'deep fakes' – disinfo's new and more-powerful apps', EUObserver, 28 December 2022, https://euobserver.com/digital-eu/156482.
167 As predicted in Giles K., Hartmann K. and Mustaffa, M. (2019), 'The Role of Deepfakes in Malign Influence Campaigns', NATO Strategic Communications Centre of Excellence, https://stratcomcoe.org/publications/the-role-of-deepfakes-in-malign-influence-campaigns/72.

What is more, given observation of the development of Russian information warfare techniques and practice runs, potential targets of Russian aggression were already alert to the possibility of faked calls to surrender – to the extent that countries like Sweden and Latvia include in the crisis preparedness booklets distributed to all members of the population specific instructions that such calls apparently coming from government officials should be disregarded because they will not be genuine. (Ukraine's own pre-war crisis preparedness booklet included a page on detecting disinformation, but no specific note on fake surrender instructions.)[168] In this case, too, Russia had acquired a capability but had not developed it to keep up with the evolution of information technologies taking place in the meantime.

Information effects within Russia

The isolation of Russians from outside information is a key enabler for the Russian state, since its ability to prosecute the war depends on effective measures to ensure Russia's population does not discover the truth about it, or frames that truth within a world view that makes the war acceptable or even desirable. As a result, Russia has put substantial and long-term effort into ensuring a homogeneous information space with no tolerance for unsanctioned viewpoints.[169] These efforts go far beyond the state television 'agitainment' shows that attract most attention outside Russia,[170] and instead encompass a holistic set of both defensive and proactive measures to shape and protect the information picture reaching Russians.[171]

The relative success of this programme can be judged by the continued willingness of Russians to fight on the front line, notwithstanding the significant but far from universal efforts to evade mobilization. But the Russian state's propaganda drive is not without challenges, especially in the context of unarguable setbacks in the conventional war. As noted by the Institute for the Study of War (ISW): 'The Russian MoD struggles to address unexpected Ukrainian operations because its information strategy relies on portraying the Russian invasion of Ukraine as an easy and faultless operation … [it] needs a significant amount of time to develop and spread false narratives in the Russian information space.'[172] Ukrainian tactical successes, such as strikes on airbases within Russia or occupied Crimea, present Russia with a dilemma that it has more than once resolved by blaming explosions on failures to follow safety protocols. In other words, Russia would rather promote explanations of incidents that show its own troops to be incompetent, and claim damage was self-inflicted, than admit to a Ukrainian capability to reach deep behind its lines.

---

168 Available, with partial English-language summary, at https://www.emergency-live.com/news/ukraine-a-brochure-on-what-to-do-in-case-of-emergency-or-war-advice-for-citizens.
169 Vasilyeva, N. (2022), 'Russian TV stars bite their tongues to feed Putin's propaganda machine', *Telegraph*, 19 November 2022, https://www.telegraph.co.uk/world-news/2022/11/19/inside-russias-tv-propaganda-machine-whatever-government-says.
170 Alyukov, M. (2022), 'How (Not) to Interpret Russian Political Talk Shows', *The Moscow Times*, 19 November 2022, https://www.themoscowtimes.com/2022/11/19/how-not-to-interpret-russian-political-talk-shows-a79399.
171 Giles (2016), *Handbook of Russian Information Warfare*.
172 Stepanenko, K. et al. (2022), 'Russian Offensive Campaign Assessment', Institute for the Study of War (ISW), 8 September 2022, https://www.understandingwar.org/backgrounder/russian-offensive-campaign-assessment-september-8.

Besides immediate steps such as monitoring internet activity and prosecuting people for repeating illegal news or opinions, Russia's concepts for shielding its population from the outside world include defences against fanciful methods of information attack that foreign powers are unlikely to be resourcing heavily. These include the 'psychological infection of personnel' through methods such as hypnosis, psychic projection and telepathy, and chemical and biological psychotropic weapons.[173] In public discussion of information warfare, these concepts are accompanied by the embrace of questionable theories of universality in human and social behaviour.[174] Although apparently misguided, this focus by a sector of Russian information warfare practitioners is noteworthy, because if Russia considers activities like these to be a threat, it follows logically that it will have considered how to deploy that threat against its adversaries.

Ukraine's commanders have noted the critical importance of carrying the information fight to Russia and ensuring that awareness of the consequences of the war spreads within Russia's own information space.

Ukraine recognizes the challenge. In September 2022, Ukraine's commanders noted the critical importance of carrying the information fight to Russia and ensuring that awareness of the consequences of the war spreads within Russia's own information space.[175] The Ukrainian government and civil society have tried to devise means of reaching into Russia to deliver information about the true nature and course of the war. These efforts include the establishment of a Ukrainian hotline which Russian families can call to try to get information on family members believed to have been sent to Ukraine to fight;[176] the hotline reportedly received over 6,000 calls in the first two weeks of the full-scale invasion.[177] Routes into Russian information space exploited by Ukrainian civilian volunteers include dating apps[178] and reviews posted on Google Maps.[179]

---

173 Wolfe, L. (2023), 'Russia Is Afraid of Western Psychic Attacks', *Foreign Policy*, 3 January 2023, https://foreignpolicy.com/2023/01/03/russia-western-psychic-attacks-mystics-astrology-putin-ukraine.
174 Wilde, G. (2022), 'In Russia's Information War, a New Field of Study Gains Traction', *New Lines Magazine*, 14 September 2022, https://newlinesmag.com/argument/in-russias-information-war-a-new-field-of-study-gains-traction.
175 Zaluzhnyy, V. and Zabrodskyy, M. (2022), 'Сколько может длиться эта война и как нам в ней победить' [How long this war can last and how we can win it], Ukrinform, 7 September 2022, https://www.ukrinform.ru/rubric-ato/3566431-perspektivy-obespecenia-voennoj-kampanii-2023-goda-ukrainskij-vzglad.html.
176 Sicard, S. (2022), 'Ukraine establishes hotline for concerned Russian families', *Military Times*, 28 February 2022, https://www.militarytimes.com/off-duty/military-culture/2022/02/28/ukraine-establishes-hotline-for-concerned-russian-families.
177 Shulka, S., Marquardt, A. and Streib, C. (2022), '"He said he was going towards Kyiv." Russian families turn to Ukrainian hotline in desperate search for lost soldiers', CNN, 7 March 2022, https://edition.cnn.com/2022/03/07/europe/ukraine-hotline-russian-soldiers-intl-cmd/index.html.
178 Florian, A. (2022), 'Matching with the enemy', *Elle*, 10 May 2022, https://www.elle.com/culture/career-politics/a39948084/matching-with-the-enemy-dating-apps-ukraine-russia-war.
179 Spocchia, G. (2022), '"Stop the War": Ukrainian activists target Russian businesses with bad Google reviews', *Independent*, 1 March 2022, https://www.independent.co.uk/news/long_reads/world/russia-ukraine-google-reviewes-army-b2025842.html.

In multiple instances, apparent Ukrainian actors have reached into Russia to hack media outlets and present audiences with subversive content.[180] In other cases, technical exploits by organizations backing Ukraine have delivered a reputational rather than a tactical impact. The '#OPRussia' campaign has carried out hack-and-leak operations against key Russian organizations such as the Bank of Russia, helping to erode the Russian state's reputation for cyber competence as well as exploiting the direct intelligence and influence value of the data acquired.[181]

However, none of these exploits is likely to have a substantial or widespread short-term impact in circumstances of well-established domestic information control within Russia, just as well-crafted direct messaging to Russian service personnel will be limited in its spread by the likelihood of severe reprisals for any recipient caught distributing it.[182] Overall, a combination of Russia's deliberate efforts to isolate its citizens from outside influences, those citizens' complicity with that process, and the universal effect of information bubbles limiting online users' interactions has meant that Ukraine's efforts to influence Russian public opinion have had little more success than those of any other external actor.

As the trends of isolation and elimination of alternative opinions within Russia are set to continue, reaching or influencing Russia's own population will only be more challenging in future conflicts. This, too, is not a new issue. Russia's long-standing and well-embedded systems of content control, both repressive and technical, will continue to present a substantial obstacle to adversaries seeking to deliver information to its people.

At the time of writing, however, the ongoing repercussions of the abortive armed revolt by the late Yevgeny Prigozhin's Wagner private military company in June 2023 offered additional insights into possible future developments within Russia. Russian information operations in wartime have shown themselves to be increasingly reactive rather than proactive, and actions by adversaries and unanticipated offline events have proven highly effective in negating Russian aims by disrupting pre-planned sequences of actions. The Prigozhin episode confirmed this and demonstrated three clear principles: a previously unsuspected vulnerability of Russia's domestic propaganda system, due to the fact that a significant proportion of its work is outsourced to private actors (a cause of particular irony when official Russian sources complained at Prigozhin being able to dominate media space, when that was exactly what he was contracted to do);[183] the slow reaction of the Russian state information system when presented with unexpected events; and its incapacity when Russian citizens come face to face with undeniable reality. The confused response to the Prigozhin mutiny replicated the early days of the full-scale invasion of Ukraine, when Russia's disinformation industry was also caught off-guard. Both occasions

---

180 For instance, a hack of Kommersant FM radio. Greenlightoff (@greenlightoff) via Twitter (2022), 'КоммерсантФМ взломали и сейчас в прямом эфире играет гимн Украины!!!' [KommersantFM hacked, now playing the Ukrainian national anthem live on air!], 8 June 2022, https://twitter.com/greenlightoff/status/1534484582560673792.
181 Osorio, N. (2022), 'Russia's Cyber Warfare Reputation Lies In Ruins As Anonymous Hacktivists Raid Central Bank Again', *International Business Times*, 6 June 2022, https://www.ibtimes.com/russias-cyber-warfare-reputation-lies-ruins-anonymous-hacktivists-raid-central-bank-3530912.
182 Reznikov, O. via YouTube (2022), 'Обращение Министра обороны Украины Алексея Резникова' [Address by Defence Minister of Ukraine], video, 7 October 2022, https://www.youtube.com/watch?v=GGqs-OgwTBs.
183 Scott, M. (2023), 'Why Putin should worry his propaganda machine broke down', Politico, 29 June 2023, https://www.politico.eu/article/vladimir-putin-wagner-yevgeny-prigozhin-russia-ukraine-war-propaganda.

demonstrated the difficulty of rapidly revising narratives and the time lag before domestic information outlets catch up with the new reality. This in turn indicates a possible route for exploitation for other actors wishing to reach and influence Russia's public.

Information effects: rest of the world

Among Western audiences, Ukraine has been highly successful in creating and leveraging messages of heroic defence – aided, of course, by the fact that there is no shortage of genuine material to work with.[184] The ability of Ukrainian government agencies, especially the Ministry of Defence, to achieve virality and engagement through humour has also achieved widespread admiration;[185] Ukraine appears to have comprehensively overcome the 'bureaucratic virality paradox', whereby government communications tend by default to be too stilted, clumsy or boring to be widely shared. This presents an obvious lesson to other government communications entities around the world, especially those that even in the third decade of the 21st century are struggling to adapt to the nature of the online information environment.[186]

Among Western audiences, Ukraine has been highly successful in creating and leveraging messages of heroic defence – aided, of course, by the fact that there is no shortage of genuine material to work with.

Nevertheless, even if it is true that Russia is 'losing the information war in Ukraine', as the head of GCHQ argues,[187] this is not the only place where the broader war will be won or lost. Audiences and decision-makers in the West appear to continue to underestimate the extent to which their view of the conflict is not shared by others around the world. Russia has been highly successful in presenting a far more ambivalent picture to the rest of the world, in terms of both who is to blame for the war and what is at stake in it.[188] Overcoming this framing would require far greater effort by the collective West than is visible at present. As noted by information practitioner Jakub Kalenský: 'This optimism and wishful

---

184 Romansky, S., Boswinkel, L. and Rademaker, M. (2022), *The parallel front: An analysis of the military use of information in the first seven months of the war in Ukraine*, The Hague Centre for Strategic Studies, October 2022, https://hcss.nl/wp-content/uploads/2022/10/The-Parallel-Front-HCSS-2022.pdf.
185 Srivastava, M., Miller, C. and Olearchyk, R. (2022), "Trolling helps show the king has no clothes': how Ukraine's army conquered Twitter', *Financial Times*, 14 October 2022, https://www.ft.com/content/b07224e1-414c-4fbd-8e2f-cfda052f7bb2.
186 Giles, K. (2023), *Humour in online information warfare: Case study on Russia's war on Ukraine*, Hybrid CoE Working Paper 26, 6 November 2023, https://www.hybridcoe.fi/publications/hybrid-coe-working-paper-26-humour-in-online-information-warfare-case-study-on-russias-war-on-ukraine; and Tokariuk, O. (2023), *Humour as a strategic tool against disinformation: Ukraine's response to Russia*, Journalist Fellowship Paper, Reuters Institute and University of Oxford, 7 December 2023, https://reutersinstitute.politics.ox.ac.uk/memes-morale-decoding-ukraines-comedy-arsenal-against-disinformation.
187 *The Economist* (2022), 'The head of GCHQ says Vladimir Putin is losing the information war in Ukraine'.
188 Klyszcz, I. (2023), 'It is not about 'neutrality': How the Global South responds to Russia's invasion', Heinrich Böll Stiftung, 30 January 2023, https://www.boell.de/en/2023/01/30/it-not-about-neutrality-how-global-south-responds-russias-invasion.

thinking are not only misguided but also very dangerous.'[189] Although some formal polls indicate a recognition among populations beyond the West that Russia's actions are dangerous and unacceptable,[190] the number of states around the world unwilling to condemn Russia's actions testifies to the success of Moscow's portrayal of the conflict – or its leverage in inducing other powers to acquiesce in it.[191]

This portrayal builds on narratives that were established long before February 2022, and in many cases even before the opening of active hostilities against Ukraine in 2014.[192] Long-term themes in Russian propaganda have achieved widespread buy-in around the world, such as the idea that Russia was 'encircled' by NATO, that NATO was aggressively taking over the countries of eastern Europe in order to threaten Russia, or that Ukraine was on the point of being accepted into NATO.[193] Since 2022, Russian disinformation directed beyond Ukraine has also leaned heavily on derogatory stereotypes of Ukrainians based around identity. False narratives based on attributes such as ethnicity, gender and sexual orientation aim to delegitimize Ukrainians and sow distrust of them.[194] In addition to the ubiquitous characterization of Ukrainians as Nazis,[195] Russian narratives regarding Ukrainian women seek to suggest that many have left the country in order to profit from prostitution rather than remain in Ukraine.[196] Sexual minorities are also targeted, with narratives aimed at conservative communities worldwide portraying the Ukrainian army as being run by homosexuals and therefore both unworthy of foreign support and doomed to defeat.[197]

Russian efforts to spread pro-war narratives have had an impact well beyond the West, and have been found to be trending in languages native to Iran, Nigeria, South Africa and South Asia.[198] Themes targeted at these language groups included the portrayal of Putin as a 'strongman', the promotion of solidarity between BRICS countries, and reminders of Western historical colonialism and consequent

---

189 Kalenský, J. (2023), 'Jakub Kalenský: The information war against the Kremlin is far from over', *Kyiv Independent*, 25 March 2023, https://kyivindependent.com/jakub-kalensky-the-information-war-against-the-kremlin-is-far-from-over.
190 Ritter, Z. and Crabtree, S. (2023), 'Russia Suffers Global Rebuke After Invasion', Gallup, 25 April 2023, https://news.gallup.com/poll/474596/russia-suffers-global-rebuke-invasion.aspx.
191 Al Jazeera (2023), 'UN tells Russia to leave Ukraine: How did countries vote?', 24 February 2023, https://www.aljazeera.com/news/2023/2/24/un-tells-russia-to-leave-ukraine-how-did-countries-vote; Klyszcz (2023), 'It is not about 'neutrality': How the Global South responds to Russia's invasion'.
192 Gretskiy, I. (2022), 'Russia's War in Ukraine: Russia's Propaganda War', ICDS, 9 August 2022, https://icds.ee/en/russias-war-in-ukraine-russias-propaganda-war.
193 Global Engagement Center (2023), 'Disinformation Roulette: The Kremlin's Year of Lies to Justify an Unjustifiable War', 23 February 2023, https://www.state.gov/disarming-disinformation/disinformation-roulette-the-kremlins-year-of-lies-to-justify-an-unjustifiable-war.
194 Global Engagement Center (2023), 'Gendered Disinformation: Tactics, Themes, and Trends by Foreign Malign Actors', 27 March 2023, https://www.state.gov/gendered-disinformation-tactics-themes-and-trends-by-foreign-malign-actors.
195 Li, D., Allen, J. and Siemaszko, C. (2023), 'Putin using false 'Nazi' narrative to justify Russia's attack on Ukraine, experts say', NBC, 24 February 2022, https://www.nbcnews.com/news/world/putin-claims-denazification-justify-russias-attack-ukraine-experts-say-rcna17537.
196 Detector Media (2022),'"Prostitution will save Ukraine from the default". Investigating Russian gender disinformation in social networks', 28 September 2022, https://detector.media/propahanda_vplyvy/article/203226/2022-09-28-prostitution-will-save-ukraine-from-the-default-investigating-russian-gender-disinformation-in-social-networks.
197 Detector Media (20220, 'You are either Russian or gay: exploring Russian LGBTIQ+ disinformation on social media', 18 November 2022, https://detector.media/monitorynh-internetu/article/205093/2022-11-18-you-are-either-russian-or-gay-exploring-russian-lgbtiq-disinformation-on-social-media.
198 Goldenziel, J. (2022), 'The Russia-Ukraine Information War Has More Fronts Than You Think', *Forbes*, 31 March 2022, https://www.forbes.com/sites/jillgoldenziel/2022/03/31/the-russia-ukraine-information-war-has-more-fronts-than-you-think.

untrustworthiness.[199] Even in the West, Russian efforts have not been entirely unsuccessful. Narratives, ideas and individual phrases that have been inculcated by Russian tools of influence over many years now permeate the entirety of Western political debate on the conflict, facilitated by a cohort of pro-Russian agitators and agents of influence who continue to operate largely unchallenged across a range of Western countries. Crucially for Ukraine, these ideas include the key one that impeding Russia in any way will inevitably lead to escalating conflict, quite possibly culminating in nuclear exchanges – this argument has presented a crippling constraint on Western efforts to support Ukraine and back it to victory.[200]

In order to propagate these narratives, Russia draws on a range of long-standing information tactics which in some cases have evolved under the pressures of the war and which in others remain static. Media sanctions in the EU, the UK and the US have led to the adoption of new channels for the dissemination of information. Existing assets such as embassies, diplomats and journalists have been co-opted to push propaganda, and numerous mirrored information-laundering websites and fake news outlets have been activated to reproduce Russian content and circumvent sanctions. But in other areas, existing practices have remained unchanged because no effective measures to interdict them have been taken.[201]

Russia continues to exploit opportunities to sow social division in the societies of Western nations opposed to its aggression.[202] Well-established cyber-information lines of effort have been augmented with the appearance of new targets, such as communities of Ukrainians displaced by the conflict and their hosts in Western countries.[203] Russia's exploitation (and possible instigation) of public burnings of copies of the Qur'an in Sweden has been especially impactful in the context of Turkish opposition to that country's NATO accession.[204] In 2022, Google noted an intensifying of hack-forge-leak activities by 'groups suspected to be tied to Russian intelligence services' designed to intimidate, discredit or neutralize not only Ukrainian military and government personnel but any significant figures opposing Russia's war.[205] Other investigations identified the Cold River/Seaborgium threat actor as prolifically involved in acquiring confidential material from targets for subsequent release by pro-Russian 'activists'.[206] By February 2023,

---

199 CASM Technology (undated), Message-based Community Detection on Twitter, https://files.casmtechnology.com/message-based-community-detection-on-twitter.pdf.
200 Giles, K. (2023), *Russian nuclear intimidation: How Russia uses nuclear threats to shape Western responses to aggression*, Research Paper, London: Royal Institute of International Affairs, https://doi.org/10.55317/9781784135645.
201 In the UK, for example, a National Security Act making some of these activities illegal only became law in July 2023. See GOV.UK (2032), 'National Security Bill becomes law', News story, 11 July 2023, https://www.gov.uk/government/news/national-security-bill-becomes-law--2.
202 See, for instance, Barry, E. (2022), 'How Russian Trolls Helped Keep the Women's March Out of Lock Step', *New York Times*, 18 September 2022, https://www.nytimes.com/2022/09/18/us/womens-march-russia-trump.html.
203 Miller, G., Mekhennet, S., Rauhala, E. and Harris, S. (2023), 'In wake of Ukraine war, U.S. and allies are hunting down Russian spies', *Washington Post*, 17 February 2023, https://www.washingtonpost.com/world/2023/02/17/russia-spies-europe-arrests.
204 Braw, E. (2023), 'How tolerance makes nations vulnerable', *Financial Times*, 10 August 2023, https://www.ft.com/content/0ac9e1a9-2aad-47d9-83fb-4839e9b31b33.
205 Google Threat Analysis Group (2023), 'Fog of war: how the Ukraine conflict transformed the cyber threat landscape'.
206 Satter, R., Pearson, J. and Bing, C. (2022), 'Exclusive: Russian hackers are linked to new Brexit leak website, Google says', Reuters, 25 May 2022, https://www.reuters.com/technology/exclusive-russian-hackers-are-linked-new-brexit-leak-website-google-says-2022-05-25.

the lead time between original hack and 'leak' on public-facing websites was greatly reduced, perhaps because the pro-Russian activists no longer saw value in plausible deniability.[207]

Similarly, Russia's transition to a less sophisticated pattern of attacks in technical cyber terms was partially mirrored in information activities against the West, with a September 2022 report by US tech conglomerate Meta describing 'an attempted smash-and-grab against the information environment, rather than a serious effort to occupy it long-term'.[208] This may have reflected a perceived loss of advantage in the course of the conflict overall: one authoritative assessment holds that Russian information warfare practitioners 'don't know how to behave when they don't have the initiative', a theory supported by the Prigozhin experience described above.[209]

Other elements of Russia's information campaigns directed at the West have evolved with the war through phases with distinct messaging components. Narratives that have come and (sometimes) gone include: the 'Winter Is Coming' campaign, intended to convince Europeans that they would freeze without Russian energy and should pressure their governments to stop backing Ukraine; the false portrayal of President Zelenskyy as a deeply corrupt leader benefiting directly from Western financial backing that would be better spent on domestic problems; the need to 'denazify', 'demilitarize' or 'desatanize' Ukraine; and most pervasively of all, the idea that continued or increased supplies of weapons to Kyiv will extend the war rather than shorten it. This latter deceptive message has been embraced by some of the most vociferous pro-Russian voices in Western countries. It has the dual advantages of tapping into a normal human desire among the broader population to shorten rather than prolong the conflict, and of directly targeting a critically important line of support for Ukraine.[210] In addition to persistent themes, Russian messaging includes specific and direct threats intended to shape the behaviour of Ukraine and its backers – among examples were the threats in August 2022 to destroy the Zaporizhzhia nuclear power station and trigger a Europe-wide radiological incident.[211]

In some cases, disinformation at the unsophisticated end of the spectrum has caused the removal of Russian state media from the platforms they previously exploited for dissemination to Western audiences. After years of complaints that disinformation operations were not only operating on social media platforms but generating substantial revenue from their advertising programmes,[212] in March 2022 Google 'pause[d] monetization and globally block[ed] recommendations' for

---

207 See, for example, Corera, G. (2023), 'SNP MP Stewart McDonald's emails hacked by Russian group', BBC News, 8 February 2023, https://www.bbc.co.uk/news/uk-politics-64562832; and Murray, C. (2023), 'I Have Stewart McDonald's Emails', craigmurray.org.uk, 10 February 2023, https://www.craigmurray.org.uk/archives/2023/02/i-have-stewart-mcdonalds-emails.
208 Nimmo, B. and Torrey, M. (2022), 'Taking down coordinated inauthentic behavior from Russia and China', Meta, September 2022, https://about.fb.com/wp-content/uploads/2022/10/CIB-Report_-China-Russia_Sept-2022-1-1.pdf.
209 Senior practitioner speaking under the Chatham House Rule at the 'Phoenix Challenge' information warfare conference, London, 1 March 2023.
210 See, for instance, 'NO2NATO NO2WAR' at https://www.no2nato.org.
211 Motyl, A. (2022), 'Russia Just Made a Threat to Destroy Europe's Largest Nuclear Power Plant: Report', 19FortyFive, 8 August 2022, https://www.19fortyfive.com/2022/08/russia-just-made-a-threat-to-destroy-europes-largest-nuclear-power-plant-report.
212 Dave, P. and Bing, C. (2019), 'Russian disinformation on YouTube draws ads, lacks warning labels -researchers', Reuters, 7 June 2019, https://news.trust.org/item/20190607064241-yi6he.

Russian state and state-aligned disinformation channels.[213] Google subsequently applied the same measures to attempts to circumvent the blocks using duplicate sites and domains.[214] However, such measures have had little impact on operations not overtly linked to the state. Social media platforms continue to present an open playground for manipulation by actors unhampered by legal or ethical constraints,[215] and the reduced enforcement on Twitter, now rebranded as X, makes that platform in particular an environment that is even more permissive for Russia and hostile for its critics.[216] In addition, Russian information operations continue to produce imitation versions of genuine established news media,[217] their effects augmented by the continued promotion of an exhaustive list of Russian talking points by news outlets in the US with substantial audiences.[218]

Publicly discernible Western efforts to counter Russia's influence appear to have been limited to the Euro-Atlantic area. Even there, the pattern of initiatives does not suggest that they are guided by an overall strategic vision or desired end state. The unprecedented extent of disclosures of information based on classified intelligence by the US and UK in the period before February 2022, for instance, led to successes at an operational level combined with negative second-order strategic effects that may not have been sufficiently appreciated in planning. Success came in preventing Russian narratives about the conflict from taking greater hold among Western publics and decision-makers than they might otherwise have done, and in pre-empting Russian false flag operations.[219] According to John Kirby, at the time a spokesperson for the US Department of Defense, the benefit of declassifying and disclosing intelligence was to 'really affect the decision-making process of a potential adversary. We were beating Putin's lie to the punch, and we know that by doing so we got inside his decision-making loop'.[220] At the same time, because this demonstration of awareness of Russia's plans was not accompanied by any credible evidence of intent to oppose them, it did nothing to deter Russia from mounting the new invasion; in fact, it provided reassurance to Moscow's assessment that there would be no meaningful response from the West.

The clear conclusion is that in addition to care over their crafting and delivery, Western strategic communications efforts need to have clear and specific aims that are developed strategically and holistically, including consideration of side effects and second-order effects.

---

213 Skibinski, M. (2022), 'Despite promises, Google and other ad platforms are still funding Russian disinformation', NewsGuard, 7 March 2022, https://www.newsguardtech.com/special-reports/ads-russian-propaganda.
214 Google Threat Analysis Group (2023), 'Fog of war: how the Ukraine conflict transformed the cyber threat landscape'.
215 Perez, C. and Nair, A. (2022), 'Information Warfare in Russia's War in Ukraine', *Foreign Policy*, 22 August 2022, https://foreignpolicy.com/2022/08/22/information-warfare-in-russias-war-in-ukraine.
216 Orr Bueno, C. (2023), 'Twitter exec says "hundreds of thousands" of Russian disinformation accounts still active on Twitter', Weaponized Spaces, 13 February 2023, https://weaponizedspaces.substack.com/p/twitter-exec-says-hundreds-of-thousands; Atanesian, G. (2023), 'Twitter staff cuts leave Russian trolls unchecked', BBC News, 14 April 2023, https://www.bbc.co.uk/news/technology-65067707.
217 European External Action Service (EEAS) (2023), *1st EEAS Report on Foreign Information Manipulation and Interference Threats: Towards a framework for networked defence*, February 2023, https://www.eeas.europa.eu/eeas/1st-eeas-report-foreign-information-manipulation-and-interference-threats_en.
218 Saletan, W. (2022), 'Fox News: Putin Propaganda Primetime', The Bulwark, 5 October 2022, https://www.thebulwark.com/fox-news-putin-propaganda-primetime.
219 Cordon, G. (2022), 'UK spy agency had to "pre-bunk" Russian propaganda over Ukraine war, GCHQ boss says', *Independent*, 29 December 2022, https://www.independent.co.uk/news/uk/home-news/jeremy-fleming-gchq-ukraine-russia-b2253045.html.
220 Banco et al. (2023), '"Something Was Badly Wrong": When Washington Realized Russia Was Actually Invading Ukraine'.

05
Lessons observed

Cyber and information operations during Russia's war on Ukraine highlight essential lessons for possible future conflict. These include the critical need for whole-of-society resilience, the role of private industry in cyber defence, and the importance of understanding Russia's distinctive information confrontation doctrine.

In theory, the study of information operations in Ukraine should provide valuable operational lessons for Ukraine's Western backers in the same way that analysis of conventional operations does, whether or not the lessons are then acted on.[221] The experience of open conflict involving a near-peer cyber power ought to validate or disprove a great deal of prior theorizing about the nature of cyber conflict, as well as the value of cyber and information power overall. In practice, the lessons observed from Ukraine are not universal: specific features of the war mean that not every lesson from it will transfer seamlessly to consideration of future clashes between Russia and other nations, including NATO allies. This chapter therefore draws together observations from the conflict broken down by key themes, and assesses whether they may be relevant for guiding preparations by NATO allies and partners for both current and future defence against Russia.

Resilience and opposition

Russia's conventional military performance in Ukraine has fallen far short of expectations. But in the cyber and information domains, Russia's failure to achieve many of its objectives appears to have as much to do with the presence of active and dynamic opposition as with Russia's own shortcomings in planning, foresight or allocation of resources.

221 Bo Lillis, K. and Liebermann, O. (2023), 'How Ukraine became a testbed for Western weapons and battlefield innovation', CNN, 16 January 2023, https://edition.cnn.com/2023/01/15/politics/ukraine-russia-war-weapons-lab/index.html.

In the wider world, this presents a striking difference from previous information operations in which Russia often achieved success through shooting at open goals because the target had little interest in defending itself. Russia's performance in the cyber and information domains also fits a broader pattern of geopolitical interaction, where Russia fails in its ambitions if it encounters determined opposition.[222] As described by Sir Jeremy Fleming, outgoing chief of the UK's GCHQ signals intelligence agency, 'Ukraine has shown that the defender has agency'[223] – this has been a key determinant in the country's continued survival.

However, Ukraine has also maximized its benefits from a set of unique advantages in the conflict. Legislative agility has enabled the rapid adaptation of the legal framework to meet novel requirements that have arisen as a result of the war, such as legalizing the evacuation of state data and beginning to regularize the status of the 'IT Army' of volunteer cyber activists. Necessity has also led to technical invention, allowing Ukraine to shortcut design and procurement processes to introduce new capabilities that many Western countries would have taken years to approve, adopt and roll out.[224]

Ukraine also has not only the benefit of understanding the language, doctrine and mental construct of its aggressor, but also the experience of almost a decade of watching Russia wage war.[225] Specifically, Ukraine learned much from being in effect a live firing range for Russian cyber capabilities over a period of years. This provided Ukraine and its backers with the opportunity both to acquire a deep understanding of Russian operations and to harden systems and infrastructure against them. As the February 2022 invasion loomed, this preparedness facilitated measures to disperse and evacuate crucial services and data to make them harder targets for kinetic attacks, and – to an extent that is debated – provide resilience in communications so that anticipated attacks on systems such as Viasat did not trigger catastrophic failures.

Ukraine also benefited from foreign support in opposing Russian information measures directed at other audiences around the world. This was decisive in the Euro-Atlantic area in countering Russia's strategic information campaign to prepare for war. Intelligence disclosures by Western powers ensured not only that Russia's justifications for the war were pre-emptively countered and false flag operations neutralized in advance, but also that the invasion did not take most Western governments – with the exception of sceptical disbelievers such as France and Germany – by surprise. However, the evolution of patterns of support for Ukraine, along with ambivalence to the war around the world, indicates that even greater efforts are needed to win the information confrontation with Russia in the Global South.

---

222 See Giles, K. (2021), *What deters Russia: Enduring principles for responding to Moscow*, Research Paper, London: Royal Institute of International Affairs, https://www.chathamhouse.org/2021/09/what-deters-russia.
223 Khalaf, R. (2023), 'GCHQ's Jeremy Fleming: "Xi doesn't want to see Putin humiliated"', *Financial Times*, 26 May 2023, https://www.ft.com/content/7979924f-dfa3-4da2-adda-23c1dceda41c.
224 Schechner, S. and Michaels, D. (2023), 'Ukraine Has Digitized Its Fighting Forces on a Shoestring', *Wall Street Journal*, 3 January 2023, https://www.wsj.com/articles/ukraine-has-digitized-its-fighting-forces-on-a-shoestring-11672741405.
225 de Liedekerke, A. and de Rivoire, H. (2022), 'Ukraine's cyber resistance is impressive – but hard to replicate', EUObserver, 26 September 2022, https://euobserver.com/opinion/156126.

Support from private enterprise

Russia continues to benefit from the success of its long-term information campaigns around the world, but in the cyber domain it is Ukraine, not Russia, that has friends in the fight. Ukraine has backing not only from friendly states, but also – perhaps even more crucially – from private enterprise. Major information technology corporations have concluded not only that they have a vested interest in ensuring security against attacks, but also that they can make a clear choice on values.

In contrast to any other domain of warfighting, in cyber and to some extent information operations, the entire domain is owned and controlled by private companies. The aspect of this in Ukraine that was not anticipated was that these private companies chose a side; and unlike in jungle or arctic warfare, where operating conditions are neutral and affect the performance of each combatant equally, the nature of the domain as a whole can be influenced to favour one party to the conflict or the other.[226] This meant that in Ukrainian cyber operations, the entire domain became a hostile environment for the aggressor. In addition, the nature of the conflict has meant that commercial actors have entered the battlefield directly and independently, rather than the more common model of being contracted by a state party to the conflict to provide support services.

In contrast to any other domain of warfighting, in cyber and to some extent information operations, the entire domain is owned and controlled by private companies.

In Ukraine, private sector corporations are providing capabilities and capacity that the government cannot. However, this presents a key advantage to Ukraine that may not be available to other states defending themselves against aggression in the future. If corporations decided to charge the full cost of their services to the victim – or indeed, not to offer their services at all – this would present a radically different set of choices to the current situation, where Ukraine benefits from many services offered on a *pro bono* basis or subsidized by friendly states.

In short, 'unlike in classical models of shooting wars where armed forces compete against each other to control territory, conflicts that have a cyber dimension involve operating in computer networks that are controlled by private companies – and these companies have a significant ability to shape the outcome of those operations'.[227] Ukraine's interaction with Starlink drives home the message that it is critical to consider the extent to which any country can or should rely on a corporate entity, which is subject to an entirely different set of constraints and motivations, in matters of war and national survival.

---

226 Giles, K. and Hartmann, K. (2018), 'Net Neutrality in the Context of Cyber Warfare', 2018 10th International Conference on Cyber Conflict, June 2018, https://www.ccdcoe.org/uploads/2018/10/Art-08-Net-Neutrality-in-the-Context-of-Cyber-Warfare.pdf.
227 Martin (2022), 'Ukraine war: US cyber chief on Kyiv's advantage over Russia'.

Perceptions and the bigger picture

Just as the offensive by Ukraine's armed forces in the autumn of 2022 gave rise to false confidence that territorial and military gains would continue and the end of the war might be close, so successes in information and cyber confrontation can give rise to misplaced optimism and even complacency, both among the general public of Western nations and among their elected leaders who are sensitive to the same information flows.

Russia has suffered tactical and operational reverses in technical terms, and local defeats in information confrontation, but at a strategic level it has not to date lost the information war. This presents a risk for the coalition of Western powers backing Ukraine, as a focus on local success has appeared to obscure the progress and importance of the broader, global conflict. This conflict requires Western planners to consider a longer temporal scale as well as broader conceptual and geographical horizons. Russia can and does use information warfare over decades-long timespans to achieve its objectives, through the slow erosion and corruption of resistance. Challenges to support for Ukraine based on misconceptions and false narratives fostered over the long term by Russia provide a clear example. This is not limited to fear of 'escalation' constraining weapons supplies, but also false ideas about Ukraine as a country, which prejudice the equally vital economic and political support for Kyiv. For future conflict, Western nations need to think as Russia does about strategic effects that are long-term, not immediate.

Part of combating this challenge is a public awareness function. Compared to attacks by missiles or tanks, cyber operations can be as imperceptible to ordinary citizens as a potentially lethal but odourless gas. The result is that they only reach public awareness if they succeed and something breaks or someone is unable to communicate – even then, it takes reporting by mass media, which is itself sometimes unable fully to comprehend what has occurred, to explain to the public what has happened. Consequently, success in cyber defence remains doomed to invisibility. The archetype illustrating this challenge is the Y2K bug, where enormous effort in solving the problem, with vast expenditure of time and resources, was rewarded with the public largely believing that because there were next to no adverse consequences, there must have been no problem to begin with.

Greater effort should be applied to deliver the message to Western publics that success in defence – of the kind seen in Ukraine – takes preparation, resources and constant effort. But this awareness is also challenged by both secrecy and obscurity surrounding cyber activities. Secrecy because the nature of many targeted institutions – military and government agencies but also banks and financial institutions – leads them to be discreet about their areas of strength and vulnerability. Obscurity because the nature of cyber operations renders them largely incomprehensible and inexplicable to most of the population. The challenge of raising awareness among the general public, or decision-makers without technical knowledge, was illustrated by a Microsoft report cited repeatedly in this paper.[228] Aimed at raising understanding among non-specialists, the report was then criticized by specialists for not including supporting evidence or 'professional estimative

228 Microsoft (2022), *Defending Ukraine: Early Lessons from the Cyber War*.

language'.[229] This demonstrates the continuing challenge of reconciling very different and perhaps incompatible communication needs for different audiences: technically oriented reporting for professionals; and simple, generic explanations for the public and, to some extent, decision-makers.

Cyber operations in war

For most of Russia's conventional forces, the full-scale invasion of Ukraine in February 2022 marked a new phase of the conflict – but not in cyberspace. Measures that would be expected from Russia during what it defines as the 'initial period of war' had either already been undertaken long before, or – as noted earlier – were not taken at all, because of a misplaced assumption that no real war would be fought.

It may be true that, in general, 'the idea of cyber operations being a competitive alternative to kinetic measures to cause decisive, large-scale, long-lasting and destructive effects has been exaggerated'.[230] But the experience of Ukraine may lead to the realization that once military operations are under way, the exercise of cyber power is just one tool among many, and the circumstances under which it will be the decisive one are far more limited.[231] Cyber effects, potentially dramatic when considered in peacetime, recede in relative significance in the context of high-intensity warfare.[232] The primary effects of cyber operations are instead integrated and cumulative: 'The question is less how a single wiper has influenced the 2022 invasion of Ukraine, and more how the persistent use of disruptive cyber capabilities has provided strategic value to Russian war efforts.'[233] Despite Russia's strategic failure, based on a fundamentally flawed appraisal of the situation in Ukraine in February 2022, this framing allows an appreciation of the distinctive benefits that cyber operations have brought to the Russian war effort, particularly in the fields of disinformation, deception, distraction and demoralization. Cyber capabilities are also a key element of Russia's ambition to achieve information isolation for control and indoctrination of its own population, as described above (see Chapter 4).

Furthermore, the fact that attitudes to the escalatory nature of cyberattacks are still not fully determined in an international context means that they are potentially of greatest utility during notional peacetime, when more direct interventions such as firing a missile are not an option but when a cyberattack can be launched without necessarily going to war. However, the example of Ukraine illustrates that when cyber is integrated as part of a warfighting toolkit, it may not necessarily deliver the game-changing effect in purely military terms that has been widely ascribed to it, because simpler and more direct methods of achieving the same

---

229 Smalley (2022), 'Cybersecurity experts question Microsoft's Ukraine report'.
230 Rõigas (2022), 'Bits versus Bombs: Observations on Russian Offensive Cyber Operations in Ukraine'.
231 Elcano Royal Institute (2022), 'The Cyberwar That Never Was: Reassessing Choices During Cyber Conflicts – Analysis', Eurasia Review, 17 July 2022, https://www.eurasiareview.com/17072022-the-cyberwar-that-never-was-reassessing-choices-during-cyber-conflicts-analysis.
232 Lyngaas, S. (2022), 'Russian missile strikes overshadow cyberattacks as Ukraine reels from blackouts', CNN, 5 November 2022, https://www.cnn.com/2022/11/05/politics/russia-cyber-attacks-missiles-ukraine-blackouts/index.html.
233 Kaminska, Shires and Smeets (2022), *Cyber Operations during the 2022 Russian invasion of Ukraine: Lessons Learned (so far)*.

outcome are no longer off the table in unrestrained conflict. Based on observation of operations in Ukraine, this has led to the following conclusion in some analysis of active hostilities: 'Probably, the most important wartime cyber-activity, on both sides, is that aimed at intelligence gathering or psychological warfare rather than destruction.'[234] This, too, highlights how considering cyber operations as a direct alternative for kinetic options is just one aspect – a very limited one – of the range of applications for cyber activities as conceptualized by Russia and as implemented on an ongoing basis against its Western adversaries.[235]

Once conflict is under way, any notional role of cyber operations as a substitute for conventional attack falls away and the question is more of the extent to which cyber effects can be integrated in a combined-operations plan – including, as necessary, targeting centres of sustainment (like stores, depots or production facilities) for advantage in an extended attritional conflict.[236] As noted above, the extent of direct coordination between information and kinetic operations by Russia remains open to question, but campaigning in Ukraine has confirmed in action the conceptually integrated nature of Russian information warfare, spanning the boundaries of espionage, destruction, and instrumentalization of information – an impression fully supported by the nature of the Vulkan contracts described above, encompassing all of these activities and more.[237] According to Microsoft: 'The lessons from Ukraine call for a coordinated and comprehensive strategy to strengthen defenses against the full range of cyber destructive, espionage, and influence operations. As the war in Ukraine illustrates, while there are differences among these threats, the Russian Government does not pursue them as separate efforts and we should not put them in separate analytical silos.'[238] In particular, information aspects of the war on Ukraine argue strongly against treating social media as the centre of gravity of disinformation efforts while ignoring other elements, such as the human (like agents of influence) and the technical (like platform-wide censorship, information interdiction, or disruptive attacks on cyber-physical systems for cognitive effect).[239]

The progress of operations in Ukraine not only highlights the interdependence of cyber and information activities. It also demonstrates the interdependence of both of these types of activity with physical events and infrastructure, and with the actions and decisions of human beings. A simple example is the dependence of telecommunications on the power grid. In circumstances where the adversary is deliberately targeting power generation and transmission – as Russia did in Ukraine in the autumn of 2022 – delivery and servicing of emergency generator or battery power to thousands of telecoms sites and data centres becomes an essential cybersecurity priority and a major and largely unanticipated logistical challenge.

---

234 *The Economist* (2022), 'Lessons from Russia's cyber-war in Ukraine'.
235 Lane. G. (2023), 'Operationalizing Deterrence by Denial in the Cyber Domain', *Military Cyber Affairs*, Vol. 6, Iss. 1, Article 4, https://doi.org/10.5038/2378-0789.6.1.1093, available at https://digitalcommons.usf.edu/mca/vol6/iss1/4.
236 Kostyuk and Gartzke (2022), 'Why Cyber Dogs Have Yet to Bark Loudly in Russia's Invasion of Ukraine'; Rõigas (2022), 'Bits versus Bombs: Observations on Russian Offensive Cyber Operations in Ukraine'.
237 Timberg, C. et al. (2023), 'Secret trove offers rare look into Russian cyberwar ambitions', *Washington Post*, 30 March 2023, https://www.washingtonpost.com/national-security/2023/03/30/russian-cyberwarfare-documents-vulkan-files.
238 Microsoft (2022), *Defending Ukraine: Early Lessons from the Cyber War*.
239 Bradshaw, S. and Denardis, L. (2022), 'Internet Infrastructure as an Emerging Terrain of Disinformation', Centre for International Governance Innovation, 4 July 2022, https://www.cigionline.org/articles/internet-infrastructure-as-an-emerging-terrain-of-disinformation.

None of the aspects of information confrontation described in this paper can be considered in isolation from its dependencies in the physical world – whether this means cyber operations relying on control of network infrastructure, or cognitive operations dependent on a willing or susceptible human audience. In this respect, the integration of both private industry and volunteer civilian efforts into both information and cyber activities during wartime raises serious questions of legal status and exposure to risk that should, as far as possible, be resolved. Legal stipulations – including the finding that 'existing international legal rules and principles already provide a workable legal framework that significantly limits the deployment of information operations by states and non-state actors'[240] – will be as irrelevant to Russian decision-making in the information domain as in any other, but they are a vital component of ensuring that Ukraine, or any other future victim of Russian aggression, retains the moral high ground. As such, they represent a key enabler for maintaining international support.

Outlook

In public commentary, expectations periodically arise not only of a renewed intensity of cyber conflict within Ukraine itself[241] but also of potential greater risk of spillover to its Western partners.[242] It should be remembered that promises of escalation from Russia are constant. As ever, a real and genuine uptick in activity by Russia directed beyond Ukraine would have to be distinguished from the constant background noise of threats of action[243] – including those made as a direct response to comments by General Nakasone on US operations in support of Ukraine.[244] However, current public assessments do not allow us to arrive at a clear conclusion over the extent of new Russian cyber capabilities that could be brought to bear in the event of direct conflict between Russia and one or more NATO states.

Assessments vary as to whether Russia has kept substantial manpower, resources and capabilities in reserve for a conflict it considers to be more important – in the same way that it has kept reserves of specific naval, air and non-conventional military capability – or whether it has in fact demonstrated the extent of its cyber power in Ukraine itself (and in operations already under way against Kyiv's coalition of backers) and there is little more that would be evidenced in a future conflict. Public debate has seen a significant quantity of evidence-free analysis on both sides of the argument, at times with a strength of conviction on the subject matched only by the paucity of verifiable data on which that conviction is based.

---

240 Dias, T. (2023), *Limits on Information Operations under International Law*, NATO Cooperative Cyber Defence Centre of Excellence, June 2023, pp. 345–64, https://www.ccdcoe.org/uploads/doc/CyCon_2023_book_print.pdf.
241 Sakellariadis and Miller (2023), 'Ukraine gears up for new phase of cyber war with Russia'.
242 Watts, C. (2023), 'Is Russia regrouping for renewed cyberwar?', Microsoft, 15 March 2023, https://blogs.microsoft.com/on-the-issues/2023/03/15/russia-ukraine-cyberwarfare-threat-intelligence-center.
243 Smalley, S. (2022), 'Russia escalates threats against West in response to cyberattacks', Cyberscoop, 9 June 2022, https://www.cyberscoop.com/russia-escalates-threats-against-west.
244 Isakova, T. and Tishina, Y. (2022), 'МИД РФ видит угрозу прямого киберстолкновения с США' [Russian MFA sees threat of direct cyber clashes with US], *Kommersant*, 6 June 2022, https://www.kommersant.ru/amp/5392410.

Even apparently well-informed assessments can vary widely, however. One line of argument is that a minority group of Russian cyber units is carrying out sophisticated cyber operations in Ukraine: a 'cyber militia' is conducting the majority of attacks there, while the main body of Russia's cyber power is held in reserve preparing for cyberwar against NATO.[245] Some senior Western government cyber officials agree that 'Russia is almost certainly capable of cyberattacks of greater scale and consequence than events in Ukraine would have one believe',[246] while the Netherlands' intelligence and security services have stated that 'the potential of cyber operations cannot be fully exploited by Russia' – without explaining further.[247]

More aggressive use of cyber capabilities against Ukraine's Western backers is a potential route for escalation by Russia if it considers this will be helpful in deterring support for Kyiv.

More aggressive use of cyber capabilities against Ukraine's Western backers is a potential route for escalation by Russia if it considers this will be helpful in deterring support for Kyiv.[248] Microsoft noted in June 2022 that 'Russia has been careful… to confine destructive "wiper software" to specific network domains inside Ukraine itself'.[249] It is reasonable to assume that lifting that restraint would pose a significant cyber challenge to Western powers. It was noted above that the Viasat hack has been assessed as having required substantial planning and preparation, which supports the idea that Russia's cyber forces were better prepared for the new invasion than its ground troops were. An alternative interpretation is that this was just one of a number of off-the-shelf attacks long prepared and kept in reserve – implying that other countries' communications infrastructure might also be at risk from Russia pending an escalation of confrontation.

It may be true that Russia has achieved less success in the information domain than anticipated within Ukraine itself.[250] However, in information as in other aspects, the conflict in Ukraine is just the front line of a much broader global contest. Seen from this perspective, outcomes in Ukraine are at most of operational significance. Strategically, the Western community of nations has far fewer grounds for optimism for the long term.

Ukraine may not be a good 'test case' for the development of cyber conflict theory for several reasons laid out in this paper: primarily, because cyber effects delivered by Russia may look different in the context of a war for which Russia has planned, targeting territory and populations it wishes to punish or damage rather than seize intact. However, the war has undoubtedly provided Russia with the opportunity

---

245 Wihersaari, J. via YouTube (2023), 'Observations of the Russian Cyberwarfare during the Ukrainian War', presentation at 'Russia's war on Ukraine: strategic and operational designs and implementation' video, 6 February 2023, https://www.youtube.com/watch?v=iI-1U5kKwd8.
246 *The Economist* (2022), 'Lessons from Russia's cyber-war in Ukraine'
247 Martin (2023), 'Dutch intelligence: Many cyberattacks by Russia are not yet public knowledge'.
248 Giles (2023), *Russian nuclear intimidation: How Russia uses nuclear threats to shape Western responses to aggression*.
249 Microsoft (2022), *Defending Ukraine: Early Lessons from the Cyber War*.
250 *The Economist* (2022), 'The head of GCHQ says Vladimir Putin is losing the information war in Ukraine'.

to learn significant lessons on what is feasible and what is not in the cyber and information domain, against an adversary that has invested heavily in resilience and has friends both internationally and in industry. According to publicly released assessments by Mandiant, the GRU has learned, adapted and moved to a concept of operations 'tailored for a fast-paced and highly contested operating environment'.[251] The Mandiant authors add that 'this operational approach may be mirrored in future crises and conflict scenarios where requirements to support high volumes of disruptive cyber operations are present'.[252] With Russia's land forces severely depleted, it is plausible that the reconstitution, reconfiguration and adaptation of tactics in information war will be significantly quicker than reconstitution of the army. It follows that continuing close attention must be paid to Russia's discussion of information confrontation theory as well as implementation of information confrontation practice, in order to have as clear an understanding as possible of what to expect in the next iteration of Russia's wars.

But the key universal lesson for any other country that may find itself the target of Russian aggression in the future is preparedness, including not only resilience at home but also building strong relationships with powerful allies and private industry. As the head of the UK's NCSC put it in late September 2022, 'you can choose how vulnerable you can be to attacks'.[253] Ukraine's resilience and continued survival have clearly demonstrated the immense value of making the right choice.

251 Black, D. and Roncone, G. (2023), 'The GRU's Disruptive Playbook', Mandiant blog, 12 July 2023, https://www.mandiant.com/resources/blog/gru-disruptive-playbook.
252 Ibid.
253 Chatham House (2022), 'Security and Defence Conference 2022: Speech, Lindy Cameron, CEO of the National Cyber Security Centre'.

06 Policy recommendations

Western policymakers need to take a number of steps to secure their countries against Russian cyber and information warfare threats. These steps include clarifying the role of private industry, recognizing the vulnerabilities of civilian information infrastructure and personal data, and pre-emptively neutralizing Russia's information assets in target countries.

The observations about the war on Ukraine outlined in the preceding chapters lead to the following recommendations for other states and coalitions seeking to defend themselves effectively against Russia in the information domain in the future:

Involvement of the private sector

— Private sector technology companies have had unprecedented direct involvement in hostilities in Ukraine. This provides them with unique (although not uniform) advantages in terms of situational awareness and visibility into current and evolving threats, but also raises significant legal, financial and security challenges. Western governments must address these challenges not only for the current level of support to Ukraine to be sustained, but also to ensure that the necessary legal and policy measures are in place in advance for any future conflict. Partly, this is to remove doubt over the combatant status of private technology companies, and to ensure the legal risks associated with their involvement in cyber aspects of war are properly understood and mitigated.

- It is vital for national governments to ensure they have full and holistic awareness of their own dependence – and their country's wider dependence – on private sector entities providing cybersecurity. Governments will need mitigating strategies to deal with the loss or absence of these entities in the event of war or conflict.
- This implies the need for the establishment in advance of engagement strategies in the event of future wars, for example: establishing which side a private sector entity is expected to, or is likely to, support; whether to withdraw products from belligerents; and how to deal with disrupted or blocked global supply chains.
- In addition, crisis-planning exercises at national and international level must integrate players from (or representing) private industry, so that industry's dominant role in the operating domain can be replicated appropriately.
- Engagement of industry must recognize the private sector constraints of accountability to shareholders, boards, regulatory bodies and employees. Support, especially if over the long term, should ordinarily be paid for in order to remove key disincentives for all but the largest industry players to get involved. The protracted duration of support to Ukraine offers a reminder that private sector commitments can be onerous.
- Industry support has been crucial for Ukraine, but it is a short-term emergency fix, not a substitute for essential organic security and resilience measures. (These are outlined in the 'Cyber power' section below.)
- Compliance requirements for private technology industries should include appropriate recognition of business continuity needs under all circumstances – up to and including armed conflict involving the physical loss of assets and networks.

Cyber power

- The success claimed by the US, and endorsed by Ukrainian counterparts, in pre-emptively strengthening Ukrainian networks before February 2022 suggests a validation of the proactive US 'defend forward' approach to identifying and eliminating threats on partner networks.[254] Pre-emptive detection and mitigation of threats have proven an essential element of successful cyber defence in conflict, and should be replicated elsewhere by stronger partners in coalitions with a shared interest in cybersecurity.
- Measures like these should augment, rather than replace, traditional security precautions, which include: ensuring network resilience through countermeasures such as maintaining patching cycles; vulnerability management; employee/civic awareness; hardware and software supply chain management; effective and agile system and data back-up; data protection and data recovery procedures for essential or sensitive data; and organic pre-emptive targeted defence such as threat intelligence measures and penetration testing.

254 US Cyber Command (2022), 'CYBER 101 – Defend Forward and Persistent Engagement', 25 October 2022, https://www.cybercom.mil/Media/News/Article/3198878/cyber-101-defend-forward-and-persistent-engagement.

- Russia's continuing eagerness to leverage the perception that responsibility for cyberattacks is difficult or even impossible to attribute should not be allowed to impede accountability. The development of public-facing threat analysis during the current phase of the conflict should be sufficient to persuade Western policymakers that – subject to appropriate caveats and application of probability language – misplaced doubts over attribution should not be a serious obstacle to holding Russia or other state or non-state threat actors accountable for their activities in cyberspace.
- The specific Ukrainian experience of managing cybersecurity for widely dispersed assets, some of which have been overrun by enemy forces, argues for default remote access to systems for security purposes – following the pattern of mass enabling of controlled folder access in Microsoft Defender. It also underlines the need for a network-centric control system for cybersecurity based on multiple control and decision-making centres to enable agile adjustment to rapidly moving events and realities of territorial control.

Dependencies

- Western governments must reassess their resilience plans – and, where these exist, comprehensive or total defence strategies – to ensure they take full account of the interdependencies highlighted by Russia's cyber and information operations against Ukraine.
- These interdependencies include the way cyber operations do not take place in a vacuum, but instead are heavily dependent on and conditioned by their environment. This means not only networks, but also their supporting physical and power infrastructure, plus consideration of who owns this infrastructure, and the organizational, legal, environmental and other considerations that influence its management and security.
- Examples of further critical dependencies include ownership and management of airwaves for data transmission, or integrity of the supply chain for hardware, software and infrastructure. These dependencies, too, need to be considered in Western resilience plans and defence strategies.
- Finally, Western governments must plan in advance for mitigating vulnerabilities to Russia's use of interlinked cyber and information operations. This must include putting in place defences and responses both for the Russian tactic of information interdiction and for the repeated pattern of following up a cyberattack with information operations to maximize the second-order psychological impacts. Western planners must recognize that technical capacities alone are not sufficient to defend against the Russian cyber-information threat; they must be accompanied by full understanding of the nature of the aggressor and the breadth of Russia's tools and intent.

Strategic communications

- NATO allies may continue the practice of selective release of classified material for pre-emptive information effect. But if so they must recognize that while highly valuable for the purpose of shaping narratives or discrediting enemy information operations, this process is ineffective for deterrence unless accompanied by a clear and credible commitment to delivering adverse consequences for the enemy if the deterrent message is not heeded.
- The vital importance of engagement with the world beyond the West to ensure protection of the rules-based international order in the face of revanchist threats has been recognized. This must now be followed up with action: Western states must invest in targeted, tailored, meaningful outreach and engagement to ensure other states recognize the nature of Russia's war on Ukraine and the implications of such wars for their own security.
- Strategic communications planners in Western states must include proactive as well as reactive elements in their shaping of the information environment, both for domestic information security and for protecting external relations with coalition partners and supporters. Those states must also step up defensive information security measures, on the basis that long-term campaigns of subversion and malign influence need to be countered before they achieve their aims, not afterwards.

Resilience

- Western states – in particular those within physical reach of Russian ground forces – should reassess their plans for national defence to account for Russia's treatment of information both as a tool and as a target. This should include the following specific considerations:
  - Critical information nodes – including data, internet and telecommunications installations as well as media and broadcasting facilities – are targets for capture and exploitation. As such, measures must be put in place for them to be destroyed rather than used by the adversary, whether pre-emptively through physical destruction, or remotely through pre-installed software payloads after they have been overrun.
  - Critical data cannot remain on systems that risk being overrun, and instead must be pre-emptively evacuated or removed to the cloud. This will entail hard choices as to what is 'critical', given the immense volumes of data daily generated by government operations. This also implies a need for adjustment to protocols and policy (including legal regimes on data protection) to cover the relocation, evacuation or destruction of critical national information systems.
  - Personal information must be recognized as a vital asset and key target for adversary operations. Capture of personal data can have lethal consequences, so such data should be protected accordingly. This protection should

go beyond the data security legislation commonly adopted in Western states for ensuring privacy, and instead envisage defence against hostile nation-state acquisition and exploitation.

- States that have received large influxes of Russian immigration since February 2022 should take an interest in the activities of these populations and enhance counter-intelligence and counter-subversion screening of their new residents. Destination states, as well as NATO nations with existing Russian diaspora populations, should study Ukraine's experience of detecting numerous bases of operations for information activities across the country, set up by Russia in advance of the full-scale invasion, and assess their own vulnerabilities to similar threats.
- Western countries with less well-developed systems of civil defence should follow the lead of front-line states in educating their populations on the actions to be taken in crisis situations, including as the result of nation state cyberattacks. The roles of key officials and civil society leaders in crisis must be clear, communicated and confirmed through exercises in advance of that crisis. Where possible, these exercises should include decision-makers from commercial entities that are critical to the functioning of society.
- Regardless of physical distance from Russia, all states must recognize the threat of Russia-backed media and proxies in information space. Even where countries are constitutionally incapable of banning such actors as Ukraine did, addressing the role of proxies, front organizations and information launderers in subversion of their host countries should be a counter-intelligence priority.

Coalitions and alliances

- NATO needs to decide properly whether 'cyber' is part of its remit or not. Private industry has been able to assist a country under attack in ways that many NATO countries, and the organization itself, would not currently be capable of doing. Article 5 of the North Atlantic Treaty appears to have had a deterrent effect on destructive Russian cyber operations against NATO member states that are directly linked to Russia's war aims in Ukraine, but there is cause to doubt whether this effect would stand a robust test. That doubt should be removed.
- Western nations with a shared vision of cybersecurity should act on it by establishing or reinforcing coalitions of the willing in cyberspace. Operations in Ukraine provide a proof of concept for a collective cyber defence architecture that is not dependent on NATO or any other currently existing formal alliance. Cooperation can and should go far beyond information sharing, and encompass both defensive and offensive joint operations, which the experience of Ukraine shows is possible without leading to the direct involvement of third countries in conventional warfare. A key part of this cooperation should be pre-emptive capacity-building: both for resilience ahead of a crisis and for capacity to absorb a surge of assistance once the crisis is under way.

Wartime conditions

- Technology companies, as well as governments, must consider the real-world effects of cyber targeting of assets they may not previously have considered to be 'military' targets, such as IP cameras or the personal information of private citizens.
- Governments, corporate entities and civilians must all give urgent consideration to the legal status of civilians and private sector organizations supporting defence information and cyber operations during hostilities. As a minimum, those individuals and organizations should be educated on the implications of their activities for their protected status as non-combatants.
- However, no plan or strategy for defence against Russia, whether militarily or politically, in peacetime or war, should rely on an expectation that Russia will abide either by international law or by any of the specific treaties, agreements and regulatory regimes to which it has notionally committed itself.
- Contributors to publicly released Western cyber and information doctrine should consider whether their current concepts of operations relate primarily to conditions below the threshold of armed conflict. If so, these concepts may require substantial revision to reflect the very different environment of open warfare.
- In particular, this revision should account for the fact that cyber activities can no longer be considered solely part of an intelligence contest, given the demonstration in Ukraine that they are likely to have a direct operational impact. Crucially, this impact is not limited to their destructive capability. Cyber power does not constitute a like-for-like replacement for conventional munitions, but it can be a force multiplier when used in combination with other information activities.
- Finally, observation of the use of information during Russia's war on Ukraine confirms that information security – to include cybersecurity – must be broadly reconceptualized in many Western states to recognize the holistic, integrated and whole-of-society nature of the threat.

About the author

Keir Giles is a senior consulting fellow with the Russia and Eurasia Programme at Chatham House in London, and also works with the Conflict Studies Research Centre, a group of subject matter experts formerly part of the UK Ministry of Defence.

Keir has studied the exploitation of the internet by hostile actors for over two decades. He combines a technical background with in-depth study of authoritarian regimes' approaches to information security to develop analysis and prediction of the development of information warfare, including the subdomain of cyber conflict. He is the author of a number of studies on Russian theory, doctrine and structures for engaging in information and cyber confrontation.

Keir is widely published on the topic of Russian military and non-military power projection. His most recent book is *Russia's War on Everybody: And What it Means for You* (Bloomsbury, 2022), which examines the human impact of Russia's cyber, information and subversion campaigns.

Acknowledgments

This product was made possible through funding and support provided by the Russia Strategic Initiative of U.S. European Command in Stuttgart, Germany.

Essential support within Chatham House came from editor Jake Statham, and from Russia and Eurasia Programme director James Nixey, assistant director Ľubica Polláková and coordinator Melania Parzonka.

The text was substantially revised following consultation with a multinational, multi-disciplinary group of experts on cybersecurity and information warfare. Particular thanks are due to Nataliya Tkachuk, Secretary of the National Cybersecurity Coordination Centre of Ukraine; Sydney Jones, Head of Cyber Threat Intelligence – CIB Americas, BNP Paribas; Valentyn Petrov, Head of the Main Situational Centre, National Security and Defence Council of Ukraine; Dan Black, Principal Analyst Cyber Espionage Team, Mandiant; Alexandra Pavliuc, Researcher, Oxford Internet Institute; Fanta Orr, Microsoft; James Shires, International Security Programme, Chatham House; and Kit Palmer, SecAlliance. Further refinements to the text were assisted by Gavin Wilde of the Carnegie Endowment for International Peace and Gentry Lane of ANOVA Intelligence.

In addition, peer reviewers from a range of countries, backgrounds and affiliations ensured that some misconceptions in early drafts were corrected. Nevertheless, any remaining errors of fact or interpretation remain entirely the author's.

Cover image: Emergency crews respond after a missile caused damage near Kyiv's TV Tower on 1 March 2022.
Photo credit: Copyright © State Emergency Service of Ukraine/Handout/Getty Images

ISBN 978 1 78413 589 8
DOI 10.55317/9781784135898

Cite this paper: Giles, K. (2023), *Russian cyber and information warfare in practice: Lessons observed from the war on Ukraine*, Research Paper, London: Royal Institute of International Affairs, https://doi.org/10.55317/9781784135898.

This publication is printed on FSC-certified paper.
designbysoapbox.com

Independent thinking since 1920

This publication was funded by the
Russia Strategic Initiative, U.S. European Command

The Royal Institute of International Affairs
Chatham House
10 St James's Square, London SW1Y 4LE
T +44 (0)20 7957 5700
contact@chathamhouse.org | chathamhouse.org

Charity Registration Number: 208223