POLITICO
Morning Cybersecurity
Delivered daily by 10 a.m., Morning Cybersecurity examines the latest news in cybersecurity policy and politics.

ne Morning Cybersecurity Newsletter

Your email...

By signing up you agree to receive email newsletters or alerts from POLITICO. You can unsubscribe at any time. This site is protected by reCAPTCHA and the Google Privacy Policy and Terms of Service apply.

DNC server feud resurfaces in impeachment battle

By **TIM STARKS** | 01/21/2020 10:00 AM EST

With help from Eric Geller, Martin Matishak and John Hendel

Editor's Note: This edition of Morning Cybersecurity is published weekdays at 10 a.m. POLITICO Pro Cybersecurity subscribers hold exclusive early access to the newsletter each morning at 6 a.m. Learn more about POLITICO Pro's comprehensive policy intelligence coverage, policy tools and services at www.politicopro.com.

QUICK FIX

— **The latest back-and-forth between the White House and House Democrats on impeachment** features some jousting over the president's remarks on the hacked DNC server.

— **Cyber Command gave itself good grades in one of its most ambitious military cyber operations,** Operation Glowing Symphony, internal documents released today found.

— **Top DHS officials in recent days offered their perspective on cyber threats** from Russia, China and Iran.

HAPPY TUESDAY and welcome to Morning Cybersecurity! Send your thoughts, feedback and especially tips to tstarks@politico.com. Be sure to follow @POLITICOPro and @MorningCybersec. Full team info below.

DRIVING THE DAY

CEASELESS SERVER SILLINESS — The White House on Monday doubled down on the discredited claim that Ukraine hacked the DNC in 2016, suggesting that President Donald Trump was right to request Ukrainian President Volodymyr Zelensky's help in investigating the conspiracy theory during their now-infamous phone call. Democrats seized on Trump's reference to the DNC server in the July 25 call as evidence of the president's fixation on a debunked right-wing talking point meant to boost his reelection prospects. But in a brief filed as part of the Senate impeachment trial, the White House said Democrats were wrong to claim that by exploring the possibility of Ukrainian hacking, Trump was dismissing Russian hacking.

"That convoluted chain of reasoning is hopelessly flawed," the brief contended. "Simply asking about any Ukrainian involvement in the 2016 election — including with respect to hacking a DNC server — does not imply that Russia did not attempt to interfere with the 2016 election." The administration further argued that Trump's pursuit of the conspiracy theory "benefits the United States by laying bare all foreign attempts to meddle in our elections," adding, "it is entirely possible that foreign nationals from more than one country sought to interfere in our election by different means (or coordinated means), and for different reasons."

House Democrats rejected many of the White House's arguments in their own filing, and they singled out another one of Trump's cyber-related beliefs for special censure. Key to the "Ukraine hacked the DNC" conspiracy theory are the notions that (a) a Ukrainian oligarch owns the cybersecurity firm CrowdStrike and (b) CrowdStrike conducted the DNC intrusion. There is "no factual basis" for those beliefs, the House said,

citing testimony by former NSC aide Fiona Hill and former homeland security adviser Tom Bossert, the latter of whom described the entire narrative as "not only a conspiracy theory" but one that "is completely debunked."

IT WAS NO 'OPERATION RAMSHACKLE JUG BAND' — An internal U.S. Cyber Command review of a cyber offensive operation against ISIS that began in 2016 concluded the mission was a success that "imposed time and resource costs" on the terrorist group's propaganda, according to documents released this morning by George Washington University's National Security Archive. In partially redacted documents obtained via a Freedom of Information Act request, Cyber Command dubbed Operation Glowing Symphony the "most complex offensive cyberspace operation USCYBERCOM has conducted to date."

The documents also revealed significant coordination in the operation. "Perhaps most importantly to the evolution of USCYBERCOM, Operation GLOWING SYMPHONY exercised the command's ability to operate at scale while coordinating with combatant commanders, other US agencies, and coalition partners," the Archive's summary of the documents concludes.

ISN'T IT IRONIC? — SafeBreach Labs discovered a ransomware technique that abuses a Windows built-in file encryption feature for business users to, well, encrypt victim devices with ransomware, the company revealed this morning. Researchers called it a sign of how ransomware can move in an "alarming new direction," and warned that "many security offerings from major Windows endpoint security vendors are affected."

FAMOUS LAST WORDS — Acting DHS Secretary Chad Wolf on Friday said the U.S. government is ready to defend the 2020 election from Russian interference. "As we saw in 2016, we fully expect Russia to attempt to interfere in the 2020 elections to sow public discord and undermine our democratic institutions. Let me be clear: We are prepared," according to prepared remarks Wolf gave at an event hosted by the Homeland Security Experts Group.

"More importantly, the state and local officials who run our elections are prepared," Wolf said, adding that DHS would once again create classified and unclassified "election war rooms" connected to "election officials in all 50 states, political parties, social media companies," the FBI, DoD and the intelligence community. Wolf admitted that even though leaders have been "laser-focused" on election security, "100 percent security is never realistic." He noted that feds are working to bolster the country's election systems and encouraging states to conduct audits of paper ballots. In 2020, "over 90 percent of votes will have a corresponding paper ballot. This is a significant achievement," Wolf said.

— ALSO, DHS TALKS IRAN, CHINA THREATS: In the same speech, Wolf said "China is our most persistent nation state threat in the cyber realm," primarily due to its cyber espionage but also because of its information operations. On Iran, he said, "We remain especially vigilant regarding cyber-enabled attacks from Iran against a range of U.S.-based targets — including our critical infrastructure," according to his prepared remarks.

On a podcast and subsequently on Twitter, DHS CISA Director Chris Krebs discussed timing of Iranian cyber retaliation over the killing of Gen. Qassem Soleimani. "The truth here is that if the Iranians were going to do something, they would probably — it was already too late," Krebs said. "If they were going to do something cyber — cybery — they would probably already be in a position and take the shot. We saw that they really didn't." Later, though, he specified that he meant attacks that depended on access for immediate retribution.

GET SMARTER ABOUT THE WORLD IN 2020: Sick of the onslaught of global news? POLITICO's man about town Ryan Heath is here to help with "Global Translations," a weekly guide that cuts through the maze of global news. He promises no "news vegetables," rather a sharp and fun newsletter that you'll love seeing arrive in your inbox. Don't miss out on this fun and enlightened read, launching on January 30. **SUBSCRIBE TODAY.**

WHITE HOUSE

MORE WHITE HOUSE CYBER TURMOIL — Two key White House cyber-related positions are reportedly getting a shakeup. The NSC's senior director for European and Russian affairs, Andrew Peek, was placed on administrative leave and apparently escorted out of the building, amid a security-related investigation. His predecessors in the job, Tim Morrison and Fiona Hill, testified in the House impeachment inquiry. Morrison held the position for a handful of months before leaving in October, making way for Peek.

Also on the move: Rear Adm. Peter Brown, Trump's third counterterrorism and homeland security adviser. Bloomberg reported he's being shifted out of the role he took on last summer to oversee Puerto Rico's recovery from natural disasters, although the position he held has seen less cybersecurity responsibility of late.

ON THE EVE OF DAVOS CONFERENCE — The World Economic Forum's Global Risks Perception Survey ranked cyberattacks and data fraud/theft among the top 10 risks. The larger Global Risks Report 2020 that contains the survey, released over the weekend, also warns about cyberattacks and their potential impact on the economy: "The current lack of global technology governance and the presence of cybersecurity blind

spots increase the risk of a fragmented cyberspace and competing technology regulations." A collection of related documents further offers advice to global leaders on cyber and more.

SENATE STALL FOR HUAWEI RIP-AND-REPLACE FUNDS — Over a month has passed since Sen. Mike Lee (R-Utah) blocked Senate Commerce Chairman Roger Wicker's attempt to fast-track House-passed legislation, H.R. 4998, authorizing $1 billion in funding to reimburse rural wireless carriers that replace gear from companies deemed a national security risk (i.e. Chinese telecom giants Huawei and ZTE). Lee's big concern: where lawmakers are getting the money (he prefers the Senate approach, which would pay for a $700 million fund via airwaves sale revenue).

But no resolution appears imminent as the Senate kicks off its impeachment trial. "We haven't heard from Wicker or his staff but we are very happy to work with them if they reach out," a Lee spokesman told Morning Tech on Friday. Wicker (R-Miss.) earlier this month, however, suggested an interest in hashing out the differences with Lee and said he didn't think the Senate would resort to scheduling a roll-call vote to bypass Lee's objections. Wicker also expressed some frustration with the process: "There's something to be said for scheduling a bill, bringing it up for amendments, taking a couple days and letting the majority speak. We're going to be in trouble if we become a body where one member has veto authority over every issue."

And Huawei is watching the legislation closely, as one exec said recently on C-SPAN, predicting that congressional action could dictate its future U.S. layoffs.

TWEET OF THE WEEKEND — Why???

POLITICO's ENERGY PODCAST : A new, daily five-minute update on the latest in energy and environmental politics and policy - must-know stories and candid insights from POLITICO's 10-person energy team and journalists across our newsroom. Subscribe for free and start listening today.

QUICK BYTES

— DOJ thinks highly of the prospects for passing encryption legislation. The Washington Post

— Some at the FBI are uneasy about Attorney General William Barr's encryption push. The Wall Street Journal

— The current dispute between Apple and the FBI and how much the company needs to help, via The New York Times.

— The U.S. is still too vulnerable to hack-and-leak election security woes, a DOJ official said. CyberScoop

— The FBI warned last month of a big hike in Ryuk attacks on municipalities. Rolling Stone

— "The FBI said in a flash security alert that nation-state actors have breached the networks of a US municipal government and a US financial entity by exploiting a critical vulnerability affecting Pulse Secure VPN servers." BleepingComputer.com

— DOJ shuttered WeLeakInfo. CyberScoop

— Just a half-million server and router passwords leaked, that's all. ZDNet

— Citrix released its first patches for a big flaw. BankInfoSecurity

— Hackers are exploiting that Citrix flaw, though, in an unusual way. CyberScoop

— Hackers are also exploiting an Internet Explorer flaw. TechCrunch

— Travelex is still having issues. BBC

— "Can the 5G network be secured against spying?" Financial Times

— Ending privacy as we know it? The New York Times

— Pensacola, Fla., isn't sure whether personal information was compromised during its recent cyberattack. WEARTV

— "A Georgia man who co-founded a service designed to protect companies from crippling distributed denial-of-service (DDoS) attacks has pleaded to paying a DDoS-for-hire service to launch attacks against others." Krebs on Security

That's all for today.

Stay in touch with the whole team: Mike Farrell (mfarrell@politico.com, @mikebfarrell); Eric Geller (egeller@politico.com, @ericgeller); Mary Lee (mlee@politico.com, @maryjylee) Martin Matishak (mmatishak@politico.com, @martinmatishak) and Tim Starks (tstarks@politico.com, @timstarks).

Follow us on Twitter

Mike Farrell @mikebfarrell
Tim Starks @timstarks
Eric Geller @ericgeller
Martin Matishak @martinmatishak

FOLLOW US

About Us
Advertising
Breaking News Alerts
Careers
Credit Card Payments
Digital Edition
FAQ
Feedback
Headlines
Photos
POWERJobs
Press
Print Subscriptions
Write For Us
RSS
Site Map

Terms of Service
Privacy Policy

© 2020 POLITICO LLC