Computer Hacks in the Russia-Ukraine War

Kenneth Geers
Very Good Security
7 Sep 2022

I. INTRODUCTION

Information is life. Therefore, when nations go to war, information operations – including data theft, denial, and manipulation – are one of the keys to victory.[1] Even in peacetime, governments today run thousands of computer network operations (CNO) every day, to support a wide range of law enforcement and intelligence actions. In some countries, they support democracy and human rights. In others, they target and terrify innocent civilians.

In 2015, while I was a visiting professor at Taras Shevchenko National University in Kyiv, I edited a book entitled *Cyber War in Perspective: Russian Aggression against Ukraine*. Twenty authors, including the chief of Ukraine's Computer Emergency Response Team (CERT-UA), detailed many cases of CNO against Ukraine's government, private sector, and civil society, specifically during the 2014 Revolution of Dignity and Russia's subsequent invasion of Crimea and Donbas.[2]

This paper examines the publicly-known CNO during Russia's further invasion of Ukraine in 2022. It describes pro-Russia and pro-Ukraine attacks, and seeks to place them into geopolitical context.

II. PRO-RUSSIA HACKS

A. Prepping the Battlespace

On Feb 24, 2022, Russia invaded Ukraine from the north, east, and south, seeking to overthrow the government of Ukrainian President Volodymyr Zelensky. Russian government hackers had been preparing for this day for at least a year, via the collection of strategic intelligence and the prepositioning of

[1] "Cyberspace Operations," Joint Publication 3-12, US Joint Chiefs of Staff, 8 Jun 2018, https://www.jcs.mil/Portals/36/Documents/Doctrine/pubs/jp3_12.pdf.
[2] *Cyber War in Perspective: Russian Aggression against Ukraine*, Kenneth Geers (Ed.), NATO Cooperative Cyber Defence Centre of Excellence (CCD COE) Publications, 2015, https://ccdcoe.org/library/publications/cyber-war-in-perspective-russian-aggression-against-ukraine/.

destructive malware. Microsoft alone detected at least six Russian "Advanced Persistent Threat" actors[3] and at least eight malware families[4] that were focused on these goals.

As over 150,000 Russian forces encircled Ukraine in early 2022, Russian CNO shifted to intimidation and destruction. Over 70 Ukrainian government websites were "defaced," and their original content was replaced with overt threats, written in Ukrainian, Russian, and Polish.[5] In mid-January, security researchers discovered WhisperGate, a malware campaign focused on encrypting files, corrupting a computer's Master Boot Record, and displaying a fake ransom note.[6]

Russian state hackers also began targeting the natural resources of Ukraine – and the United States (US). On Jan 14, Oleg Nykonorov, CEO of Regional Gas Company, announced on Facebook that his IT staff were fighting "like lions" to defend their enterprise.[7] In mid-Feb, hackers likely associated with Russia's Main Intelligence Directorate (GRU) gained access to over 100 computers associated with 21 US liquefied natural gas (LNG) companies, paying up to $15,000 per account on the dark web, and used them as a backdoor into company networks. These attacks showed foresight, as Russia's pending war would skyrocket the demand for LNG worldwide, especially from the US.[8]

For ten days prior to the invasion (Feb 15-24), Russian CNO shifted again, to distributed denial-of-service (DDoS) attacks. The Ukrainian government announced that the attacks, which targeted ministries, intelligence agencies, and banks, were the largest DDoS it had ever seen. In such cases, attacker attribution is often a slow process, but on Feb 18, the White House announced that it possessed "technical information" linking the attacks to the GRU.[9]

---

[3] In this paper, "Advanced Persistent Threat," or APT, is synonymous with a team working with or for a nation-state intelligence agency.
[4] "Special Report: Ukraine An overview of Russia's cyberattack activity in Ukraine," Microsoft Digital Security Unit, 27 Apr 2022, https://query.prod.cms.rt.microsoft.com/cms/api/am/binary/RE4Vwwd.
[5] "More than 70 Ukrainian government websites have been defaced in cyberattacks," Jenna McLaughlin, NPR, 19 Jan 2022, https://www.npr.org/2022/01/19/1074172805/more-than-70-ukrainian-government-websites-have-been-defaced-in-cyber-attacks.
[6] "Destructive malware targeting Ukrainian organizations," Microsoft Security, 15 Jan 2022, https://www.microsoft.com/security/blog/2022/01/15/destructive-malware-targeting-ukrainian-organizations/.
[7] Oleg Nykonorov, 14 Jan 2022, Facebook post, https://www.facebook.com/photo/?fbid=669565037387751&set=a.215320962812163.
[8] "Hackers Targeted U.S. LNG Producers in Run-Up to Ukraine War," Jordan Robertson and Sergio Chapa, Bloomberg, 7 Mar 2022, https://www.bloomberg.com/news/articles/2022-03-07/hackers-targeted-u-s-lng-producers-in-run-up-to-war-in-ukraine.
[9] "Press Briefing by Press Secretary Jen Psaki, Deputy National Security Advisor for Cyber and Emerging Technology Anne Neuberger, and Deputy National Security Advisor for International Economics and Deputy NEC Director Daleep Singh," The White House, 18 Feb 2022, https://www.whitehouse.gov/briefing-room/press-briefings/2022/02/18/press-briefing-by-press-secretary-jen-psaki-deputy-national-security-advisor-for-cyber-and-emerging-technology-anne-neuberger-and-deputy-national-security-advisor-for-international-economics-and-dep/.

B. H-Hour

On Feb 24, as Russian troops attempted to take Kyiv, Russian CNO shifted again, this time to destructive "wiper" code that targeted the Ukrainian government. On Feb 23, HermeticWiper/FoxBlade appeared, in a highly tailored deployment that included a signed digital certificate.[10] On Feb 24, malware analysts discovered IsaacWiper; this attack was so urgent that a new version was released within two days.[11]

One of this war's biggest hacks occurred exactly one hour before the Russian army crossed into Ukraine. A likely malicious firmware update in Viasat ground infrastructure rendered the US firm's KA-SAT modems unusable.[12] The Ukrainian military uses Viasat for military command-and-control (C2); therefore, the attack had an "immediate and significant" impact on Ukrainian government communications.[13] As with NotPetya in 2017, there was collateral damage across Europe, including over 5,000 wind turbines in Germany. The US Government attributed the Viasat hack to Russia.[14]

Ukrainian communications were a key target on the opening day of the war. On Feb 24 (and then again on Mar 9), hackers penetrated Triolan, a major Ukrainian Internet service provider, and succeeded in resetting devices to factory settings. The attackers destroyed "key nodes" of the company's network, and some routers could not be recovered. Mitigation was a challenge because the restoration of some equipment required physical access, which became more difficult once the war started.[15]

On Feb 24, the Russian army invaded the Ukrainian border town of Sumy. In a subsequent report, Microsoft noted that suspected Russian hackers had been active on Sumy's critical infrastructure networks since at least Feb 17.[16] On Mar 3, there was a telecoms blackout in the Sumy Oblast, followed by regional power outages, explosions at an electricity substation, and explosions at a combined heat and power (CHP) plant in Sumy, resulting in a loss of heat, water and electricity.[17]

---

[10] "HermeticWiper | New Destructive Malware Used In Cyber Attacks on Ukraine," Juan Andrés Guerrero-Saade, Sentinel Labs, 23 Feb 2022, https://www.sentinelone.com/labs/hermetic-wiper-ukraine-under-attack/.
[11] "IsaacWiper and HermeticWizard: New wiper and worm targeting Ukraine," ESET Research, 1 Mar 2022, https://www.welivesecurity.com/2022/03/01/isaacwiper-hermeticwizard-wiper-worm-targeting-ukraine/.
[12] "A Mysterious Satellite Hack Has Victims Far Beyond Ukraine," Matt Burgess, *WIRED*, 23 Mar 2022, https://www.wired.com/story/viasat-internet-hack-ukraine-russia/.
[13] "Russia hacked an American satellite company one hour before the Ukraine invasion," Patrick Howell O'Neill, *MIT Technology Review*, 10 May 2022, https://www.technologyreview.com/2022/05/10/1051973/russia-hack-viasat-satellite-ukraine-invasion/.
[14] "Attribution of Russia's Malicious Cyber Activity Against Ukraine," Antony J. Blinken, U.S. Department of State, 10 May 2022, https://www.state.gov/attribution-of-russias-malicious-cyber-activity-against-ukraine/.
[15] "As Russia Invaded, Hackers Broke Into A Ukrainian Internet Provider. Then Did It Again As Bombs Rained Down," Thomas Brewster, *Forbes*, 10 Mar 2022, https://www.forbes.com/sites/thomasbrewster/2022/03/10/cyberattack-on-major-ukraine-internet-provider-causes-major-outages/?sh=7c62e46d6573.
[16] "Special Report: Ukraine: An overview of Russia's cyberattack activity in Ukraine," Microsoft Digital Security Unit, April 27, 2022, https://query.prod.cms.rt.microsoft.com/cms/api/am/binary/RE4Vwwd.
[17] "Telecoms blackout hits northeast Ukraine; large power outages also reported," Corin Faife, *The Verge*, 3 Mar 2022, https://www.theverge.com/2022/3/3/22960374/telecoms-blackout-northeast-ukraine-power-outage-sumy.

On Feb 25, CERT-UA announced that hackers working for the Belarusian Ministry of Defense (aka UNC1151 or Ghostwriter) conducted a spearphishing campaign targeting the private email accounts of members of the Ukrainian armed forces.[18]

Once the invasion began, there was an increased focus on psychological operations (PSYOP) against Ukraine. SMS threats were sent both to soldiers ("flee or be killed") and to citizens ("ATMs are not working").[19] Ukrainian military leadership Facebook accounts were hacked, from which the hackers tried to order Ukrainian troops to surrender.[20] Facebook detected and disrupted state actors from Russia and Belarus, who were conducting influence operations on its platform.[21] Russian spam bots were repurposed from anti-vax to anti-Ukraine campaigns.[22] On 21 July, two Ukrainian radio stations were hacked, and used to spread fake messages that Zelensky had been hospitalized and was in critical condition.[23]

C. Pro-Russia Hacks: Evolution

The correlation between CNO and traditional military operations is sometimes easy to see. On Mar 1, the Russian military announced its intention to destroy "disinformation" targets in Ukraine. That same day, a Russian missile destroyed Kyiv's primary TV tower, and suspected Russian state hackers deployed DesertBlade (a malware family that overwrites data and renders machines unbootable) against a major Ukrainian broadcasting company.[24] In another case, according to Microsoft, Russia took down the computer network of a nuclear power plant before Russian troops took it over.[25]

In other cases, a bit more homework is required to see how and where new campaigns fit on existing timelines of threat actors and malware families. On Mar 15, ESET researchers discovered CaddyWiper, which did not share a code base with HermeticWiper or IsaacWiper. However, the new campaign

---

[18] "Ukraine links Belarusian hackers to phishing targeting its military," Sergiu Gatlan, *Bleeping Computer*, 25 Feb 2022, https://www.bleepingcomputer.com/news/security/ukraine-links-belarusian-hackers-to-phishing-targeting-its-military/.

[19] "Disturbing Mass Text Operation Terrorizes Ukraine as Russian Troops Move In," Shannon Vavra, *Daily Beast*, 23 Feb 2022, https://www.thedailybeast.com/cyberattacks-hit-websites-and-psy-ops-sms-messages-targeting-ukrainians-ramp-up-as-russia-moves-into-ukraine.

[20] "Hackers' fake claims of Ukrainian surrender aren't fooling anyone. So what's their goal?" Kate Conger, *The New York Times*, 5 Apr 2022, https://www.nytimes.com/2022/04/05/us/politics/ukraine-russia-hackers.html.

[21] "Adversarial Threat Report," Ben Nimmo, David Agranovich and Nathaniel Gleicher, Meta, April 2022, https://about.fb.com/wp-content/uploads/2022/04/Meta-Quarterly-Adversarial-Threat-Report_Q1-2022.pdf.

[22] "'Bot holiday': Covid disinformation down as social media pivot to Ukraine," Melody Schreiber, *The Guardian*, 4 Mar 2022, https://www.theguardian.com/media/2022/mar/04/bot-holiday-covid-misinformation-ukraine-social-media.

[23] "Ukrainian radio broadcaster hacked to spread fake news about Zelensky's health," Daryna Antoniuk, The Record by Recorded Future, 22 Jul 2022, https://therecord.media/ukrainian-radio-broadcaster-hacked-to-spread-fake-news-about-zelenskys-health/.

[24] "Special Report: Ukraine An overview of Russia's cyberattack activity in Ukraine," Microsoft Digital Security Unit, 27 Apr 2022, https://query.prod.cms.rt.microsoft.com/cms/api/am/binary/RE4Vwwd.

[25] "Many Russian Cyberattacks Failed in First Months of Ukraine War, Study Says," David E. Sanger and Julian E. Barnes, *The New York Times*, June 22, 2022, https://www.nytimes.com/2022/06/22/us/politics/russia-ukraine-cyberattacks.html.

specifically targeted Ukrainian organizations, destroyed user data, and deleted partition information on attached drives.[26] Just one week later, on Mar 22, CERT-UA released the details of yet another wiper: DoubleZero.[27]

One of the most ambitious attempts to use a wiper in this war could have caused a blackout for two million Ukrainian citizens. On March 19 – just days after Ukraine joined the Europe Union's power grid – Russian hackers (alleged to be GRU Unit 74455 or "Sandworm") are believed to have temporarily shut down nine electric substations, using "Industroyer2" malware, which can wipe Windows, Linux, and Solaris operating systems.[28] The hackers tried and failed to turn off the power and then destroy the computers used to control the electricity grid.[29]

One of the most successful attacks occurred on Mar 28, when hackers caused an extended, country-wide network disruption at the national ISP Ukrtelecom, by targeting its "core infrastructure." According to NetBlocks, Ukrtelecom suffered a drop in connectivity to just 13% of its pre-war levels. The company was only able to restore its service 15 hours after the initial disruption.[30] According to Victor Zhora of Ukraine's State Service for Special Communications and Information Protection (SSSCIP), the government was concerned that this attack was not a DDoS, but a deeper, more sophisticated intrusion.[31]

Some attacks come in clear response to ongoing geopolitical events. On Jun 27, as the Russian foreign ministry threatened to retaliate against Lithuania for halting the transit of EU-sanctioned goods to the Russian exclave of Kaliningrad, a pro-Kremlin hacking group, "Killnet," conducted a DDoS attack that it said "demolished" over 1500 Lithunian sites.[32] Lithuania's National Cyber Security Centre (NKSC) said that some users could not access the country's Secure Data Transfer Network, which was specifically built to allow government officials to communicate during crises.[33] By mid-July, Killnet had declared "war" on 10 nations that were supporting Ukraine. Its impressive Telegram channel was created just after the

---

[26] "CaddyWiper: New wiper malware discovered in Ukraine," ESET, 15 Mar 2022, https://www.welivesecurity.com/2022/03/15/caddywiper-new-wiper-malware-discovered-ukraine/.
[27] "Кібератака на українські підприємства з використанням програми-деструктора DoubleZero (CERT-UA#4243)," CERT-UA Computer Emergency Response Team of Ukraine, 22 Mar 2022, https://cert.gov.ua/article/38088.
[28] "Industroyer2: Industroyer reloaded," ESET Research, 12 Apr 2022, https://www.welivesecurity.com/2022/04/12/industroyer2-industroyer-reloaded/.
[29] "Russian hackers tried to bring down Ukraine's power grid to help the invasion," Patrick Howell O'Neill, *MIT Technology Review*, April 12, 2022, https://www.technologyreview.com/2022/04/12/1049586/russian-hackers-tried-to-bring-down-ukraines-power-grid-to-help-the-invasion/.
[30] "Internet disruptions registered as Russia moves in on Ukraine," NetBlocks, 28 Mar 2022, https://netblocks.org/reports/internet-disruptions-registered-as-russia-moves-in-on-ukraine-W80p4k8K.
[31] "'Most Severe' Cyberattack Since Russian Invasion Crashes Ukraine Internet Provider," Thomas Brewster, *Forbes*, 28 Mar 2022, https://www.forbes.com/sites/thomasbrewster/2022/03/28/huge-cyberattack-on-ukrtelecom-biggest-since-russian-invasion-crashes-ukraine-telecom/?sh=1f1838767dc2.
[32] "Russian missile strike hits shopping mall in central Ukraine — live updates," *Deutsche Welle*, 27 June 2002, https://www.dw.com/en/russian-missile-strike-hits-shopping-mall-in-central-ukraine-live-updates/a-62271288.
[33] "Pro-Russia hackers claim responsibility for 'intense, ongoing' cyberattack against Lithuanian websites," Sean Lyngaas, CNN, 27 Jun 2022, https://edition.cnn.com/2022/06/27/politics/lithuania-cyber-attack-pro-russian-group/index.html.

Russian invasion. Similar "patriotic" hackers working with XakNet, Trickbot, and Conti, are suspected to be working for or with Russian intelligence.[34]

According to Microsoft, by June 2022, Russian CNO successfully penetrated 128 networks in 42 countries, including Ukraine, the US, Poland, the Baltics, Sweden, Finland, Denmark, Norway, and Turkey. Victims included government agencies, think tanks, humanitarian groups, telecommunications, energy, and defense companies. However, Russia has also been more careful with its malware than with NotPetya in 2017, confining its worm-like behavior to specific network domains in Ukraine.[35]

In the Ukrainian territory which the Kremlin has recently captured, such as Kherson, Russia is quick to replace Ukrainian telecoms infrastructure with its own, including SIM cards with Russian numbers, so that all data is routed through Russia. Thus, many Ukrainians are now living under Russia's System for Operative Investigative Activities (SORM), which can read email, intercept text messages, censor information, and disseminate propaganda.[36] In late July, Russian state hackers disseminated an Android app called "CyberAzov," which looked like a tool to hack Russia, but in fact was malware designed to discover who would use such an app.[37]

Finally, this paper focuses on computer hacking, and not on disinformation, but there is a link between the two. Botnets spread propaganda, such as the story about secret US biological weapons laboratories in Ukraine.[38] On Aug 5, Ukrainian authorities dismantled a "million-strong" bot farm used to discredit Ukrainian leadership and to create social rifts in the country, seizing 5,000 SIM cards used to create and maintain accounts, and 200 proxy servers used to spoof IP addresses.[39]

And there is more than one way to hack information: in 2014, the Crimea campaign was buttressed by mass changes to *Wikipedia*, where Russian propaganda teams worked to drive the narrative;[40] in 2022, a Moscow court fined the Wikimedia Foundation 5 million roubles, demanding the removal of certain information in *Wikipedia* articles about Russia's invasion of Ukraine, as it posed a risk to "public order"

---

[34] "Russian 'Hacktivists' Are Causing Trouble Far Beyond Ukraine," Matt Burgess, *WIRED*, 11 Jul 2022, https://www.wired.com/story/russia-hacking-xaknet-killnet/.
[35] "Defending Ukraine: Early Lessons from the Cyber War," Brad Smith, Microsoft, 22 Jun 2022, https://blogs.microsoft.com/on-the-issues/2022/06/22/defending-ukraine-early-lessons-from-the-cyber-war/.
[36] "Russia Is Taking Over Ukraine's Internet," Matt Burgess, *WIRED*, 15 Jun 2022, https://www.wired.com/story/ukraine-russia-internet-takeover/.
[37] "Russia Released a Ukrainian App for Hacking Russia That Was Actually Malware," Lorenzo Franceschi-Bicchierai, *Motherboard*, 19 Jul 2022, https://www.vice.com/en/article/bvmnxd/russia-released-a-ukrainian-app-for-hacking-russia-that-was-actually-malware.
[38] "Russia claims U.S. labs across Ukraine are secretly developing biological weapons," Steve Inskeep and Odette Yousef, *National Public Radio*, 22 Mar 2022, https://www.npr.org/2022/03/22/1087991730/russia-claims-u-s-labs-across-ukraine-are-secretly-developing-biological-weapons.
[39] "Ukraine dismantled million-strong disinformation bot farm," Vilius Petkauskas, *Cybernews*, 5 Aug 2022, https://cybernews.com/cyber-war/ukraine-dismantled-million-strong-disinformation-bot-farm/.
[40] "Cyber Operations at Maidan: A First-Hand Account," Glib Pakharenko, in *Cyber War in Perspective: Russian Aggression against Ukraine*, Kenneth Geers (Ed.), NATO Cooperative Cyber Defence Centre of Excellence (CCD COE) Publications, 2015, https://ccdcoe.org/library/publications/cyber-war-in-perspective-russian-aggression-against-ukraine/.

in Russia;[41] and the Donetsk People's Republic (DPR) announced that it had blocked access to the Google search engine, because it promoted disinformation.[42]

III. PRO-UKRAINE HACKS

A. H-Hour

During the initial phase of Russia's invasion, one group of hackers may have played a strategic role in helping the Ukrainian government to survive. Working with Belarusian dissidents, they compromised Belarusian railway signal control cabinets (which still ran Windows XP) in an effort to sabotage Russian military deployments, transiting Belarus on their way to Ukraine. The targeted train traffic was reportedly "paralyzed" for days, and contributed to the vulnerable 40-mile convoy north of Kyiv. Belarusian police announced the capture of three saboteurs, and state television broadcast "chilling" footage of the men, still bleeding from having been shot in the knees.[43]

Typically, in war, the defender enjoys some strategic advantages, such as a superior knowledge of battlefield terrain and communication networks. Following its invasion, Russian forces struggled with both, as its forces failed to take Kyiv, and were forced to withdraw from northern Ukraine. Russian forces are believed to have suffered a breakdown in military communications, which led to a reliance on Ukrainian SIM cards. As a result, Russian comms were more vulnerable to interception, jamming, and geolocation, which may have led to the assassination of an unusually high number of senior Russian military officers.[44]

On Feb 24, the world's most famous hacktivist group tweeted: "The Anonymous collective is officially in cyber war against the Russian government." Subsequently, Anonymous claimed to have defaced or knocked offline many Russian government and media sites, doxed the Russian MoD, and hacked Russian television to display war footage from Ukraine.[45] Anonymous defaced the website of Russia's Space Research Institute (IKI), and leaked files from Roscosmos, which announced that no satellite control centers had been hacked, but that doing so might be a "cause for war."[46] The Anonymous group Squad

---

[41] "Wikipedia fights Russian order to remove Ukraine war information," Reuters, 13 Jun 2022, https://www.reuters.com/world/europe/wikipedia-fights-russian-order-remove-ukraine-war-information-2022-06-13/ .

[42] "Russian-backed separatists in Ukraine block Google search engine," Reuters, 22 Jul 2022, https://www.reuters.com/world/europe/russian-backed-separatists-ukraine-block-google-search-engine-2022-07-22/.

[43] "The Belarusian railway workers who helped thwart Russia's attack on Kyiv," Liz Sly, *Washington Post*, 23 Apr 2022, https://www.washingtonpost.com/world/2022/04/23/ukraine-belarus-railway-saboteurs-russia/.

[44] "Communication Breakdown: How Russia's Invasion of Ukraine Bogged Down," Sergei Dobrynin and Mark Krutov, *Radio Free Europe/Radio Liberty*, 19 Mar 2022, https://www-rferl-org.cdn.ampproject.org/c/s/www.rferl.org/amp/communication-lapses-russia-invasion-failures/31761259.html.

[45] "Anonymous: the hacker collective that has declared cyberwar on Russia," Dan Milmo, *The Guardian*, 27 Feb 2022, https://www.theguardian.com/world/2022/feb/27/anonymous-the-hacker-collective-that-has-declared-cyberwar-on-russia.

[46] "Hackers Breach Russian Space Research Institute Website," Joseph Cox, *VICE*, 3 Mar 2022,

303 sent millions of text messages to Russian phone numbers in an attempt to provide Russian citizens with better information about the war.[47]

B. Hacker Allies

In geopolitics, it is hard to overstate the importance of allies. Therefore, on Feb 26, the Ukrainian government issued a worldwide call for "cyber volunteers," to anyone in the world who would be willing to attack digital targets in Russia. A designated Telegram channel, "IT ARMY of Ukraine," gained nearly 300k subscribers. Assigned tasks included DDoS, propaganda, doxing, defacements, intelligence gathering, and engaging in simple political dialogue with Russian citizens. Naturally, there are significant challenges to mobilizing an army of hackers, to include vetting, command-and-control, adversary infiltration, mistakes, and possible retaliation.[48]

Clearly, some hackers have signed up for duty. One prominent example is the Distributed Denial of Secrets website, which has posted over 6 million Russian and Belarusian documents, allegedly stolen from government, military, intelligence, economic, and media domains. There were 360k files from *Roskomnadzor*, the agency responsible for monitoring, controlling, and censoring Russian mass media. Due to the ongoing war and the controversial origin of the documents, a disclaimer reminds researchers that some of the data could be fabricated, altered, or contain malware.[49]

At the nation-state level, Ukraine is likely receiving far more help from its NATO/EU allies than Russia is receiving from autocratic nation-states. Belarus is now severely dependent on the Kremlin, and on Mar 7 its Ghostwriter APT was caught installing MicroBackdoor on Ukrainian government systems.[50] China may be playing a double game: its state hackers were accused of conducting espionage against Ukraine and the West – but also against Russia and Belarus.[51] At a May 16 meeting of the Collective Security Treaty Organization (CSTO), Russia's counter to NATO, only Belarus voiced its support for Moscow's invasion of Ukraine.[52]

The US has been active and vocal in supporting Ukraine: the FBI has shared intelligence; USAID has provided thousands of emergency communication devices; and DOE is helping to integrate Ukraine's electrical grid with the EU.[53] The US DHS/Cybersecurity and Infrastructure Security Agency (CISA) "Shields Up" website has provided intelligence reports, updates, and best practices for countering Russian

https://www.vice.com/en/article/z3n8ea/hackers-breach-russian-space-research-institute-website.
[47] "Anonymous: How hackers are trying to undermine Putin," Joe Tidy, *BBC*, 20 Mar 2022, https://www.bbc.com/news/technology-60784526.
[48] "Ukraine's IT army: Who are the cyber guerrillas hacking Russia?" Janosch Delcker, *Deutsche Welle*, 24 Mar 2022, https://www.dw.com/en/ukraines-it-army-who-are-the-cyber-guerrillas-hacking-russia/a-61247527.
[49] *Distributed Denial of Secrets*, Category: Russia, https://ddosecrets.com/wiki/Category:Russia.
[50] "A deeper look at hacking groups and malware targeting Ukraine," Emma Vail, The Record by Recorded Future, 27 Apr 2022, https://therecord.media/a-deeper-look-at-hacking-groups-and-malware-targeting-ukraine/.
[51] "Mystery of alleged Chinese hack on eve of Ukraine invasion," Gordon Corera, *BBC News*, 7 Apr 2022, https://www.bbc.com/news/technology-60983346.
[52] "Russian Allies Get Tongue-Lashing at Putin's Ultimate Pity Party," Shannon Vavra, *The Daily Beast*, 17 May 2022, https://www.thedailybeast.com/allies-of-russian-president-vladimir-putin-scolded-over-ukraine-at-csto-summit.
[53] "U.S. Support for Connectivity and Cybersecurity in Ukraine," US Department of State, 10 May 2022, https://www.state.gov/u-s-support-for-connectivity-and-cybersecurity-in-ukraine/.

CNO;[54] in late July, CISA announced a new Memorandum of Cooperation (MoC) with Ukraine's SSSCIP.[55] The White House announced a preemptive counter-hacking operation that secretly removed Russian malware that had been installed around the world.[56] And while naming and shaming Russian hackers may not have improved deterrence, it is much better at building an alliance of defenders.[57]

The US Cyber Command (CYBERCOM) is collaborating with its counterpart in Ukraine.[58] In June, CYBERCOM Director General Paul Nakasone announced that the US was engaged in defensive and offensive operations, "across the full spectrum," in support of Ukraine; in response, Andrey Krutskikh, Russia's top cyber diplomat, said that Russia would respond to all such aggressive operations. Krutskikh claimed that over 65,000 "armchair hackers" from the West were taking part in DDoS attacks against Russia, and warned that such behavior increased the risk of a traditional military clash with the West. In July, CYBERCOM published a list of 20 indicators of compromise (IOC) that it had received from Ukrainian security services.[59]

In February, the European Union (EU) created a Cyber Rapid Response Team (CRRT) to help Ukraine, which was led by Lithuania; participating nations included Croatia, Poland, Estonia, Romania, and the Netherlands.[60]

C. Pro-Ukraine Hacks: Evolution

In the first days of the war, one strategic counter-hack came partly in response to the successful Russian attack on Viasat. The Ukrainian vice prime minister sent a desperate tweet to Elon Musk, who in turn green-lighted the immediate delivery of his Starlink satellite Internet service to Ukraine. Starlink's low-orbit system works in tandem with backpack-sized stations on the ground, and offers high-speed, strongly encrypted, highly configurable service, which has withstood increasingly sophisticated Russian hacks. Starlink has been used for countless military and civilian communications in this war; it keeps Zelensky in touch with allied leaders and gives Ukrainian commanders the ability to call artillery strikes on the battlefield.[61]

Naturally, InfoSec experts have been asked to opine not just on Russian CNO, but also on broader questions of national security and international relations. One expert recommended that the West send a

[54] "SHIELDS UP," Cybersecurity & Infrastructure Security Agency, https://www.cisa.gov/shields-up.
[55] "US Expands Cybersecurity Partnership With Ukraine," Danny Bradbury, *Infosecurity*, 28 Jul 2022, https://www.infosecurity-magazine.com/news/us-cybersecurity-partnership/.
[56] "U.S. Says It Secretly Removed Malware Worldwide, Pre-empting Russian Cyberattacks," Kate Conger and David Sanger, *The New York Times*, 6 Apr 2022, https://www.nytimes.com/2022/04/06/us/politics/us-russia-malware-cyberattacks.html.
[57] "The Hidden War in Ukraine," Emily Harding, Center for Strategic and International Studies, June 15, 2022, https://www.csis.org/analysis/hidden-war-ukraine.
[58] "U.S. Support for Connectivity and Cybersecurity in Ukraine," US Department of State, 10 May 2022, https://www.state.gov/u-s-support-for-connectivity-and-cybersecurity-in-ukraine/.
[59] "U.S. Posts Traces of Ukraine Hacks As Part of Cyber Alliance Against Russia," Tom O'connor, *Newsweek*, 20 Jul 2022, https://www.newsweek.com/us-posts-traces-ukraine-hacks-part-cyber-alliance-against-russia-1726429.
[60] "US Expands Cybersecurity Partnership With Ukraine," Danny Bradbury, *Infosecurity*, 28 Jul 2022, https://www.infosecurity-magazine.com/news/us-cybersecurity-partnership/.
[61] "UkraineX: How Elon Musk's space satellites changed the war on the ground," Christopher Miller, Mark Scott and Bryan Bender, *Politico*, 8 Jun 2022, https://www.politico.eu/article/elon-musk-ukraine-starlink/.

message of deterrence to the Kremlin by temporarily knocking Russia offline.[62] However, there is no guarantee that such a dramatic CNO would lead to desired political results,[63] and it may deprive the West of its own lucrative CNO. One danger might lie in the domain of nuclear command-and-control (NC3); both the US and Russia have warned that impeding either nation's NC3[64] could lead to catastrophic results.[65]

As the war grinds on, every day is a good day to hack something, as each side strives to obtain an advantage. On June 17, a DDoS attack delayed a speech by Russian President Vladimir Putin for 100 minutes. The incident took place at the St. Petersburg International Economic Forum, where Putin (eventually) gave a talk on Russian resilience in the face of Western sanctions.[66] The attack allegedly struck a database of conference participants, which complicated the process of screening guests, who included Chinese and Egyptian leadership figures.[67]

In a September interview, one group of non-state Ukrainian hackers claimed to have compromised Russian television stations to promote pro-Ukraine messages, taken control of thousands of security and traffic cameras in Belarus and occupied parts of Ukraine to geolocate Russian military personnel, and to have used fake profiles of women on Facebook and Russian social media websites to gather intelligence from Russian forces; according to the hackers, they subsequently share this information with the Ukrainian military.[68]

IV. MID-WAR ASSESSMENT

The classified nature of nation-state computer hacking ensures that open-source researchers cannot see everything. However, there are already many publicly-known examples of computer hacking in this war. And while no single CNO is likely to have a strategic impact, there is today little doubt that soldiers do not move without some type of hacker support. Microsoft alone has reported 2-3 "destructive" GRU-associated CNO in Ukraine per week since Feb 23.[69] The two most impactful hacks may have

[62] "Here's how the U.S. Should Respond to any Russian Cyberattacks," Dmitri Alperovitch and Samuel Charap, *The Washington Post*, 14 Apr 2022, https://www.washingtonpost.com/outlook/2022/04/15/us-russia-cyber-attacks/.
[63] "Ukraine Wants to Basically Kick Russia Off the Internet. Terrible Idea." Courtney Radsch, *Slate*, 3 Mar 2022, https://slate.com/technology/2022/03/ukraine-kicking-russia-off-internet-icann.html.
[64] "Cyber Signaling and Nuclear Deterrence: Implications for the Ukraine Crisis," Erica Lonergan and Keren Yarhi-Milo, *War on the Rocks*, 21 Apr 2022, https://warontherocks.com/2022/04/cyber-signaling-and-nuclear-deterrence-implications-for-the-ukraine-crisis/.
[65] ""When the Urgency of Time and Circumstances Clearly Does Not Permit . . .": Pre-delegation in Nuclear and Cyber Scenarios," Peter Feaver and Kenneth Geers, Carnegie Endowment for International Peace, 16 Oct 2017, https://carnegieendowment.org/2017/10/16/when-urgency-of-time-and-circumstances-clearly-does-not-permit-.-.-.-pre-delegation-in-nuclear-and-cyber-scenarios-pub-73417.
[66] "DDoS Attacks Delay Putin Speech at Russian Economic Forum," staff reporting, *Dark Reading*, 20 Jun 2022, https://www.darkreading.com/attacks-breaches/ddos-attacks-delay-putin-speech-russian-economic-forum.
[67] "Today's D Brief," Ben Watson, Jennifer Hlad, Bradley Peniston, *Defense One*, 17 Jun 2022, https://www.defenseone.com/threats/2022/06/the-d-brief-june-17-2022/368327/.
[68] "Hackers Honeytrap Russian Troops Into Sharing Location, Base Bombed: Report," Giulia Carbonaro, *Newsweek*, 6 Sep 2022, https://www.newsweek.com/hackers-honeytrap-russian-troops-sharing-location-base-bombed-report-1740070.
[69] "Special Report: Ukraine An overview of Russia's cyberattack activity in Ukraine," Microsoft Digital Security Unit, 27 Apr 2022, https://query.prod.cms.rt.microsoft.com/cms/api/am/binary/RE4Vwwd.

occurred at the start of the war: the pro-Russia takedown of Viasat, and the pro-Ukraine hack of Belarusian railways.

It will take some time to better grasp what this war means for our understanding of CNO. At this time, one important question is whether Russia could not destroy more Ukrainian networks (e.g. air defense or leadership comms), or whether they were kept up by design (e.g. to facilitate Russian espionage or military comms). One expert workshop held in Estonia on May 30 suggested that, in this war, we may in fact have seen the full extent of Russian cyber capabilities, while also noting that the high operational tempo of a real war would at least temporarily lead to a high burnout rate in tools, personnel, and operations.[70] One current theory is that, in January, Russia was too concerned with intimidating Ukraine via PSYOP, and thereby burned too much of its access to Ukraine's networks before the war began.[71] It is also possible that Moscow may have simply expected a quick and easy victory, which is a common political mistake throughout history. Or perhaps Ukrainian infrastructure – like the country itself – was simply too big, too diverse, and too connected to conquer.

According to Yurii Shchyhol, head of Ukraine's SSSCIP, there have been at least three difference-making gifts from the West: first, Starlink helped Ukraine to relaunch destroyed infrastructure; second, servers and mobile data centers allowed Ukraine to create backup copies of entire institutions, which allowed for the continuous operation of government; and third, since the invasion, some expensive software has been provided for free, such as an Amazon private cloud, where the government now administers data from state registries.[72]

One critical area of research is how to secure a decentralized battlefield. In the battle for Kyiv, a crowdfunded unit of drone-flying Ukrainian special forces on quad bikes successfully harassed the invaders.[73] One 15-year-old Ukrainian boy pinpointed a Russian convoy with his drone, and the footage led to the destruction of more than 20 Russian military vehicles.[74] The "Dnipro 1" drone intelligence unit can place an explosive charge of up to 800g on its craft.[75] On June 22, a drone crashed into the Novoshakhtinsk oil refinery in Rostov, Russia, causing a massive explosion, and a shutdown of the

---

[70] "Cyber Operations during the 2022 Russian invasion of Ukraine: Lessons Learned (so far)," Monica Kaminska, James Shires, Max Smeets, Tallinn Workshop Report, ECCRI Tallinn Workshop Report, July 2022, https://eccri.eu/wp-content/uploads/2022/07/ECCRI_WorkshopReport_Version-Online.pdf.
[71] "Did Russia mess up its cyberwar with Ukraine before it even invaded?" Tim Starks and Aaron Schaffer, *Washington Post*, 4 Aug 2022, https://www.washingtonpost.com/politics/2022/08/04/did-russia-mess-up-its-cyberwar-with-ukraine-before-it-even-invaded/.
[72] "The Man at the Center of the New Cyber World War," Kenneth R. Rosen, *Politico*, 14 July 2022, https://www.politico.com/news/magazine/2022/07/14/russia-cyberattacks-ukraine-cybersecurity-00045486.
[73] "The drone operators who halted Russian convoy headed for Kyiv,"Julian Borger, *The Guardian*, 28 Mar 2022, https://www.theguardian.com/world/2022/mar/28/the-drone-operators-who-halted-the-russian-armoured-vehicles-heading-for-kyiv.
[74] "Ukraine war: Teenager and father used drone to spy on Russian forces and help army," Amar Mehta, Sky News, 12 Jun 2022, https://news.sky.com/story/ukraine-war-teenager-and-father-used-drone-to-spy-on-russian-forces-and-help-ukraines-army-12632472.
[75] "Ukraine-Russia: Hidden tech war as Slovyansk battle looms," Jonathan Beale, *BBC*, 8 Jul 2022, https://www.bbc.com/news/world-europe-62090791.

plant.[76] On July 31, an apparently homemade drone carrying an explosive device detonated at the headquarters of Russia's Black Sea Fleet on the Crimean peninsula, injuring six people, and causing the cancellation of observances of Russia's Navy Day holiday.[77] On July 12, the White House said that Iran was preparing to supply Russia with drones that may have combat capabilities.[78] And even when the war is over, robot sappers will help to clear minefields.[79] However, drones in this war have been vulnerable to jamming, tracking, and destruction, with an average lifespan of just seven days.[80]

Finally, this war is not only a catastrophe for Ukraine, but also for Russia. Even from the perspective of DEF CON 30, the fact that scientists, intellectuals, and artists are leaving Russia in numbers not seen since 1917[81] means that Russia is bleeding hackers. Yandex alone, which was generally considered to be Russia's "coolest" company and its national answer to Google, has lost thousands of employees (including its CEO) since the start of the war.[82] RUNET is now a digital Iron Curtain, a self-inflicted denial-of-service, and it will take years to replenish its lost talent. The SSSCIP is now urging the West to prevent any Russian code from running on Western networks, and it is seeking the ouster of Russia from international organizations like the International Telecommunication Union (ITU).[83]

In Ukraine, the opposite appears to be happening, as the now work-from-home IT sector is apparently thriving during the war – air raid sirens notwithstanding.[84]

A. Key Observations

Here are some potential lessons from what we have seen so far:

1. Computer network defense (CND) has evolved
    a. There is hope for computer network attack (CNA) deterrence by denial
2. CNA has been disruptive but not decisive
    a. It requires a huge effort with no guarantee of results
3. Allies are key to victory

---

[76] "Drone crashes into Russian oil refinery in possible attack," Andrew Roth, *The Guardian*, 22 Jun 2022, https://www.theguardian.com/world/2022/jun/22/russian-novoshakhtinsk-oil-refinery-struck-drone-possible-attack-inside-borders.
[77] "Drone blast strikes Russia's Black Sea Fleet command," Associated Press, 31 Jul 2022, https://www.pbs.org/newshour/world/drone-blast-strikes-russias-black-sea-fleet-command.
[78] "Ukraine war: Iran plans to supply Russia with drones, US warns," *BBC*, 12 July 2022, https://www.bbc.com/news/world-us-canada-62130725.
[79] "Russia-Ukraine war: what we know on day 110 of the invasion," Samantha Lock, *The Guardian*, 13 Jun 2022, https://www.theguardian.com/world/2022/jun/13/russia-ukraine-war-what-we-know-on-day-110-of-the-invasion.
[80] "Ukraine-Russia: Hidden tech war as Slovyansk battle looms," Jonathan Beale, BBC, 8 Jul 2022, https://www.bbc.com/news/world-europe-62090791.
[81] "Who are the Russians leaving their country?" Anastassia Boutsko, *Deutsche Welle*, 5 Apr 2022, https://www.dw.com/en/who-are-the-russians-leaving-their-country/a-61364390.
[82] "How War in Ukraine Roiled Russia's 'Coolest Company," Neil MacFarquhar, *New York Times*, 6 Jul 2022, https://www.nytimes.com/2022/07/06/world/europe/ukraine-russia-yandex-google.html.
[83] "The Man at the Center of the New Cyber World War," Kenneth R. Rosen, *Politico*, 14 July 2022, https://www.politico.com/news/magazine/2022/07/14/russia-cyberattacks-ukraine-cybersecurity-00045486.
[84] "The Economy Putin Didn't Actually Ruin," David Segal, *The New York Times*, 22 Jul 2022, https://www.nytimes.com/2022/07/22/business/ukraine-tech-companies-putin.html.

    a. Ukraine has CNO support from NATO, EU, IT/InfoSec firms, hackers
4. Cyber power is soft power
    a. IT and computer hacking are more democratic than autocratic
5. Connectivity has been surprisingly resilient
    a. Ukraine and wunderkind Zelensky are still connected
6. Information operations have outshined CNA
    a. Simplicity and reach beat complexity and limits
7. Attribution is trending
    a. Government and IT firms are naming hackers in record time
8. Back your stuff up in the cloud
    a. In another country if possible
9. Decentralized warfare offers increased opportunities to attackers
    a. And defenders.

Of course, these are only preliminary thoughts. As Natasha is warned after 2,000 pages of *War and Peace*: there is still a great deal more to come.