Atlantic Council | CYBER STATECRAFT INITIATIVE | DFRLab

A PARALLEL TERRAIN:

Public-Private Defense of the Ukrainian Information Environment

Emma Schroeder

Sean Dack

CYBER STATECRAFT
INITIATIVE

DFRLab

The Cyber Statecraft Initiative works at the nexus of geopolitics and cybersecurity to craft strategies to help shape the conduct of statecraft and to better inform and secure users of technology. This work extends through the competition of state and non-state actors, the security of the internet and computing systems, the safety of operational technology and physical systems, and the communities of cyberspace. The Initiative convenes a diverse network of passionate and knowledgeable contributors, bridging the gap among technical, policy, and user communities.

The mission of the **Digital Forensic Research Lab (DFRLab)** is to identify, expose, and explain disinformation where and when it occurs using open-source research; to promote objective truth as a foundation of government for and by people; to protect democratic institutions and norms from those who would seek to undermine them in the digital engagement space; to create a new model of expertise adapted for impact and real-world results; and to forge digital resilience at a time when humans are more interconnected than at any point in history, by building the world's leading hub of digital forensic analysts tracking events in governance, technology, and security

Atlantic Council
1030 15th Street NW, 12th Floor
Washington, DC 20005

For more information, please visit
www.AtlanticCouncil.org.

CYBER STATECRAFT
INITIATIVE

DFRLab

A PARALLEL TERRAIN:

Public-Private Defense of the Ukrainian Information Environment

Emma Schroeder

Sean Dack

ATLANTIC COUNCIL

TABLE OF CONTENTS

EXECUTIVE SUMMARY

In the year since the Russian invasion of Ukraine, the conventional assault and advances into Ukrainian territory have been paralleled by a simultaneous invasion of the Ukrainian information environment. This environment, composed of cyber infrastructure, both digital and physical, and the data, networks, and ideas that flow through and across it, is more than a domain through which the combatants engage or a set of tools by which combatants interact—it is a parallel territory that Russia is intent on severing from the global environment and claiming for itself.

Russian assaults on the Ukrainian information environment are conducted against, and through, largely privately owned infrastructure, and Ukrainian defense in this space is likewise bound up in cooperative efforts with those infrastructure owners and other technology companies providing aid and assistance. The role of private companies in this conflict seems likely to grow, along with the scale, complexity, and criticality of the information infrastructure they operate.

Examining and mitigating the risks related to the involvement of private technology companies in the war in Ukraine is crucial and looking forward, the United States government must also examine the same questions with regard to its own security and defense:

1. What is the complete incentive structure behind a company's decision to provide products or services to a state at war?

2. How dependent are states on the privately held portions of the information environment, including infrastructure, tools, knowledge, data, skills, and more, for their own national security and defense?

3. How can the public and private sectors work together better as partners to understand and prepare these areas of reliance during peace and across the continuum of conflict in a sustained, rather than ad hoc, nature?

Russia's war against Ukraine is not over and similar aggressions are likely to occur in new contexts and with new actors in the future. By learning these lessons now and strengthening the government's ability to work cooperatively with the private sector in and through the information space, the United States will be more effective and resilient against future threats.

INTRODUCTION

Russia's invasion of Ukraine in 2022 held none of the illusory cover of its 2014 operation; instead of "little green men" unclaimed by Moscow, Putin built up his forces on Ukraine's border for the entire international community to see. His ambitions were clear: To remove and replace the elected government of Ukraine with a figurehead who would pull the country back under Russia's hold, whether through literal absorption of the state or by subsuming the entire Ukrainian population under Russia's political and information control. In the year since the Russian invasion, Ukraine's defense has held back the Russian war machine with far greater strength than many thought possible in the early months of 2022. President Zelenskyy, the Ukrainian government, and the Ukrainian people have repeatedly repelled Russian attempts to topple the state, buttressed in part by the outpouring of assistance from not just allied states, but also local and transnational private sector companies.

Amidst the largest conventional land war in Europe since the fall of the Third Reich, both Russia and Ukraine have directed considerable effort toward the conflict's information environment, defined as the physical and digital infrastructure over and through which information moves, the tools used to interact with that information, and information itself. This is not only a domain through which combatants engage, but a parallel territory that the Kremlin seeks to contest and claim. Russian efforts in this realm, to destroy or replace Ukraine's underpinning infrastructure and inhibit the accessibility and reach of infrastructure and tools within the environment, are countered by a Ukrainian defense that prioritizes openness and accessibility.

The information environment, and all the components therein, is not a state or military dominated environment; it is largely owned, operated, and populated by private organizations and individuals around the globe. The Ukrainian information environment, referring to Ukrainian infrastructure operators, service providers, and users, is linked to and part of a global environment of state and non-state actors where the infrastructure and the terrain is largely private. Russian operations within the Ukrainian information environment are conducted against, and through, this privately owned infrastructure, and the Ukrainian defense is likewise bound up in cooperative efforts with those infrastructure owners and other technology companies that are providing aid and assistance. These efforts have contributed materially, and in some cases uniquely, to Ukraine's defense.

The centrality of this environment to the conduct of this war, raises important questions about the degree to which states and societies are dependent on information infrastructure and functionalities owned and operated by private actors, and especially transnational private actors. Although private sector involvement in the war in Ukraine has generally been positive, the fact that the conduct of war and other responsibilities in the realm of statehood are reliant on private actors leads to new challenges for these companies, for the Ukrainian government, and for the United States and allies.

The United States government must improve its understanding of, and facility for, joint public-private action to contest over and through the information "environment" in future conflicts. The recommendations in this report are intended to facilitate the ability of US technology companies to send necessary aid to Ukraine, ensure that the US government has a complete picture of US private-sector involvement in the war in Ukraine, and contribute more effectively to the resilience of the Ukrainian information environment. First, the US government should issue a directive providing assurance and clarification as to the legality of private sector cyber, information, capacity building, and technical aid to Ukraine. Second, a task force pulling from agencies and offices across government should coordinate to track past, current, and future aid from the private sector in these areas to create a better map of US collaboration with Ukraine across the public and private sectors. Third, the US government should increase its facilitation of private technology aid by providing logistical and financial support.

These recommendations, focused on Ukraine's defense, are borne of and provoke larger questions that will only become more important to tackle. The information environment and attempts to control it have long been a facet of conflict, but the centrality of privately owned and operated technology—and the primacy of some private sector security capabilities in relation to all but a handful of states—pose increasingly novel challenges to the United States and allied policymaking communities. Especially in future conflicts, the risks associated with private sector action in defense of, or directly against, a combatant could be significantly greater and multifaceted, rendering existing cooperative models insufficient.

THE RUSSIAN INFORMATION OFFENSIVE

The Russian Federation Ministry of Foreign Affairs defines information space—of which cyberspace is a part—as "the sphere of activity connected with the formation, creation, conversion, transfer, use, and storage of information and which has an effect on individual and social consciousness, the information infrastructure, and information itself."[1] Isolating the Ukrainian information space is key to both the short- and long-term plans of the Russian government. In the short term, the Kremlin pursues efforts to control both the flow and content of communications across the occupied areas.[2] In the longer term, occupation of the information environment represents an integral step in Russian plans to occupy and claim control over the Ukrainian population.

In distinct opposition to the global nature of the information environment, over the past decade or so, the Kremlin has produced successive legislation "to impose 'sovereignty' over the infrastructure, content, and data traversing Russia's 'information space,'" creating a sectioned-off portion of the internet now known as RuNet.[3] Within this space, the Russian government has greater control over what information Russian citizens see and a greater ability to monitor what Russian citizens do online.[4] This exclusionary interpretation is an exercise in regime security against what the Kremlin perceives as constant Western information warfare against it.[5] As Gavin Wilde, senior fellow with the Carnegie Endowment for International Peace, writes, the Russian government views the information environment "as an ecosystem to be decisively dominated."[6]

To the Kremlin, domination of the information environment in Ukraine is an essential step toward pulling the nation into its fold and under its control. Just as Putin views information domination as critical to his regime's exercise of power within Russia, in Ukraine, Russian forces systematically conduct offensives against the Ukrainian information environment in an attempt to create a similar model of influence and control that would further enable physical domination. This strategy is evident across the Kremlin's efforts to weaken the Ukrainian state for the last decade at least. In the 2014 and 2022 invasions, occupied, annexed, and newly "independent" regions of Ukraine were variously cut off from the wider information space and pulled into the restricted Russian information space.

The Crimean Precedent—2014

The Russian invasion of Ukraine did not begin in 2022, but in 2014. Examining this earlier Russian incursion illustrates the pattern of Russian offensive behavior in and through the information environment going back nearly a decade—a combination of physical, cyber, financial, and informational maneuvers that largely target or move through private information infrastructure. In 2014, although obfuscated behind a carefully constructed veil of legitimacy, Russian forces specifically targeted Ukrainian information infrastructure to separate the Crimean population from the Ukrainian information environment, and thereby the global information environment, and filled that vacuum with Russian infrastructure and information.

1 The Ministry of Foreign Affairs of the Russian Federation, Convention on International Information Security (2011), https://carnegieendowment.org/files/RUSSIAN-DRAFT-CONVENTION-ON-INTERNATIONAL-INFORMATION-SECURITY.pdf.

2 To learn more about Russian disinformation efforts against Ukraine and its allies, check out the Russian Narratives Reports from the Atlantic Council's Digital Forensic Research Lab: Nika Aleksejeva et al., Andy Carvin ed., "Narrative Warfare: How the Kremlin and Russian News Outlets Justified a War of Aggression against Ukraine," Atlantic Council, February 22, 2023, https://www.atlanticcouncil.org/in-depth-research-reports/report/narrative-warfare/; Roman Osadchuk et al., Andy Carvin ed., "Undermining Ukraine: How the Kremlin Employs Information Operations to Erode Global Confidence in Ukraine," Atlantic Council, February 22, 2023, https://www.atlanticcouncil.org/in-depth-research-reports/report/undermining-ukraine/.

3 Previously, the term *RuNet* described Russian language portions of the global internet accessible anywhere in the world. However, since Russia passed a domestic internet law in May 2019, RuNet has come to refer to a technically isolated version of the internet that services users within the borders of Russia. Gavin Wilde and Justin Sherman, *No Water's Edge: Russia's Information War and Regime Security*, *Carnegie Endowment for International Peace*, January 4, 2023, https://carnegieendowment.org/2023/01/04/no-water-s-edge-russia-s-information-war-and-regime-security-pub-88644; Justin Sherman, *Reassessing Runet: Russian Internet Isolation and Implications for Russian Cyber Behavior*, *Atlantic Council*, July 7, 2022, https://www.atlanticcouncil.org/in-depth-research-reports/issue-brief/reassessing-runet-russian-internet-isolation-and-implications-for-russian-cyber-behavior/.

4 Adam Satariano and Valerie Hopkins, "Russia, Blocked from the Global Internet, Plunges into Digital Isolation," New York Times, March 7, 2022, https://www.nytimes.com/2022/03/07/technology/russia-ukraine-internet-isolation.html.

5 Gavin Wilde and Justin Sherman, *No Water's Edge: Russia's Information War and Regime Security, Carnegie Endowment for International Peace*, January 4, 2023, https://carnegieendowment.org/2023/01/04/no-water-s-edge-russia-s-information-war-and-regime-security-pub-88644; Stephen Blank, "Russian Information Warfare as Domestic Counterinsurgency," *American Foreign Policy Interests* 35, no. 1 (2013): 31–44, https://doi.org/10.1080/10803920.2013.757946.

6 Gavin Wilde, *Cyber Operations in Ukraine: Russia's Unmet Expectations, Carnegie Endowment for International Peace*, December 12, 2022, https://carnegieendowment.org/2022/12/12/cyber-operations-in-ukraine-russia-s-unmet-expectations-pub-88607.

The Russian invasion of eastern Ukraine in 2014 was a direct response to the year-long Euromaidan Revolution, which took place across Ukraine in protest of then-President Viktor Yanukovych's decision to spurn closer relations with the European Union and ignore growing calls to counter Russian influence and corruption within the Ukrainian government. These protests were organized, mobilized, and sustained partially through coordination, information exchange, and message amplification over social media sites like Facebook, Twitter, YouTube, and Ustream—as well as traditional media.[7] In February 2014, after Yanukovych fled to Russia, the Ukrainian parliament established a new acting government and announced that elections for a new president would be held in May. Tensions immediately heightened, as Russian forces began operating in Crimea with the approval of Federal Assembly of Russia at the request of "President" Yanukovych, although Putin denied that they were anything other than "local self-defense forces."[8] On March 21, Putin signed the annexation of Crimea.[9]

During the February 2014 invasion of Crimea, the seizure and co-option of Ukrainian physical information infrastructure was a priority. Reportedly, among the first targets of Russian special forces was the Simferopol Internet Exchange Point (IXP), a network facility that enables internet traffic exchange.[10] Ukraine's state-owned telecommunications company Ukrtelecom reported that armed men seized its offices in Crimea and tampered with fiber-optic internet and telephone cables.[11] Following the raid, the company lost the "technical capacity to provide connection between the peninsula and the rest of Ukraine and probably across the peninsula, too."[12] Around the same time, the head of the Security Service of Ukraine (SBU), Valentyn Nalivaichenko, reported that the mobile phones of Ukrainian parliament members, including his own, were blocked from connecting through Ukrtelecom networks in Crimea.[13]

From March to June 2014, Russian state-owned telecom company Rostelcom began and completed construction of the Kerch Strait cable, measuring 46 kilometers (about 28.5 miles) and costing somewhere between $11 and $25 million, to connect the Crimean internet with the Russian RuNet[14] Rostelcom, using a local agent in Crimea called Miranda Media, became the main transit network for several Crimean internet service providers (ISPs), including KCT, ACS-Group, CrimeaCom, and CRELCOM in a short period of time.[15] There was a slower transition of customers from the Ukrainian company Datagroup to Russian ISPs, but nonetheless, the number of Datagroup customers in Crimea greatly decreased throughout 2014. According to one ISP interviewed by Romain Fontugne, Ksenia Ermoshina, and Emile Aben, "the Kerch Strait cable was used first of all for voice communication … The traffic capacity of this cable was rather weak for commercial

7 Tetyana Bohdanova, "Unexpected Revolution: The Role of Social Media in Ukraine's Euromaidan Uprising," *European View* 13, no. 1: (2014), https://doi.org/10.1007/s12290-014-0296-4; Megan MacDuffee Metzger, and Joshua A. Tucker. "Social Media and EuroMaidan: A Review Essay," *Slavic Review* 76, no. 1 (2017): 169–91, doi:10.1017/slr.2017.16.

8 Jonathon Cosgrove, "The Russian Invasion of the Crimean Peninsula 2014–2015: A Post-Cold War Nuclear Crisis Case Study," Johns Hopkins (2020), 11–13, https://www.jhuapl.edu/Content/documents/RussianInvasionCrimeanPeninsula.pdf.

9 Steven Pifer, *Ukraine: Six Years after the Maidan, Brookings*, February 21, 2020, https://www.brookings.edu/blog/order-from-chaos/2020/02/21/ukraine-six-years-after-the-maidan/.

10 Kenneth Geers, ed., *Cyber War in Perspective: Russian Aggression Against Ukraine* (Tallinn: NATO CCD COE Publications, 2015), 9; Keir Giles, "Russia and Its Neighbours: Old Attitudes, New Capabilities," in Geers, *Cyber War in Perspective,* 25; 'Кримські регіональні підрозділи ПАТ «Укртелеком» офіційно повідомляють про блокування невідомими декількох вузлів зв'язку на півострові' [Ukrtelekom officially reports blocking of communications nodes on peninsula by unknown actors], Ukrtelekom, February 28, 2014, http://www.ukrtelecom.ua/presscenter/news/official?id=120327.

11 Pavel Polityuk and Jim Finkle, "Ukraine Says Communications Hit, MPs Phones Blocked," Reuters, March 4, 2014, https://www.reuters.com/article/ukraine-crisis-cybersecurity/ukraine-says-communications-hit-mps-phones-blocked-idINL6N0M12CF20140304.

12 Jen Weedon, "Beyond 'Cyber War': Russia's Use of Strategic Cyber Espionage and Information Operations in Ukraine," in Geers, *Cyber War in Perspective*, 76; Liisa Past, "Missing in Action: Rhetoric on Cyber Warfare," in Geers, *Cyber War in Perspective,* 91; "Ukrtelecom's Crimean Sub-Branches Officially Report that Unknown People Have Seized Several Telecommunications Nodes in the Crimea," Ukrtelecom, February 28, 2014, http://en.ukrtelecom.ua/about/news?id=120467; "Feb. 28 Updates on the Crisis in Ukraine," *New York Times*, February 28, 2014, https://archive.nytimes.com/thelede.blogs.nytimes.com/2014/02/28/latest-updates-tensions-in-ukraine/?_r=0; "The Crimean Regional Units of PJSC 'Ukrtelecom' Officially Inform About the Blocking by Unknown Persons of Several Communication Nodes on the Peninsula," Ukrtelecom, February 28, 2014, https://web.archive.org/web/20140305001208/, http://www.ukrtelecom.ua/presscenter/news/official?id=120327.

13 Polityuk and Finkle, "Ukraine Says Communications Hit"; John Leyden, "Cyber Battle Apparently under Way in Russia–Ukraine Conflict," The Register, April 25, 2018, https://www.theregister.com/2014/03/04/ukraine_cyber_conflict/.

14 Joseph Cox, "Russia Built an Underwater Cable to Bring Its Internet to Newly Annexed Crimea," VICE, August 1, 2014, https://www.vice.com/en/article/ypw35k/russia-built-an-underwater-cable-to-bring-its-internet-to-newly-annexed-crimea.

15 Cox, "Russia Built an Underwater Cable."

communications."[16] But by the end of 2017, remnant usage of Ukrainian ISPs had virtually disappeared, following the completion of a second, better internet cable through the Kerch Strait and a series of restrictions placed on Russian social media platforms, news outlets, and a major search engine by Ukrainian President Poroshenko.[17] The combination of the new restrictions, and the improved service of Russian ISPs encouraged more Crimeans to move away from Ukrainian ISPs.

Over the next three years, and through the "progressive centralization of routing paths and monopolization of Internet Service market in Crimea … the topology of Crimean networks has evolved to a singular state where paths bound to the peninsula converge to two ISPs (Rosetelecom and Fiord)," owned and operated by Russia.[18] Russian forces manipulated the Border Gateway Protocol (BGP)—the system that helps connects user traffic flowing from ISPs to the wider internet—modifying routes to force Crimean internet traffic through Russian systems, "drawing a kind of 'digital frontline' consistent with the military one."[19] Residents of Crimea found their choices increasingly limited, until their internet service could only route through Russia, instead of Ukraine, subject to the same level of censorship and internet controls as in Russia. The Russian Federal Security Service (FSB) monitored communications from residents of Crimea, both within the peninsula and with people in Ukraine and beyond.[20] Collaboration between ISPs operating in Crimea through Russian servers and the FSB appears to be a crucial piece of this wider monitoring effort. This claim was partially confirmed by a 2018 Russian decree that forbade internet providers from publicly sharing any information regarding their cooperation with "the authorized state bodies carrying out search and investigative activities to ensure the security of the Russian Federation."[21]

Russia's efforts to control the information environment within Crimea, and the Russian government's ability to monitor communications and restrict access to non-Russian approved servers, severely curtailed freedom of expression and belief—earning the region zero out of four in this category from Freedom House.[22] Through physical, and formerly private, information infrastructure, Russia was able to largely take control of the information environment within Crimea.

A Parallel Occupation—2022

Digital Information Infrastructure

Just as in 2014, one of the first priorities of invading Russian forces in 2022 was the assault of key Ukrainian information infrastructure, including digital infrastructure. Before, during, and following the invasion, Russian and Russian-aligned forces targeted Ukrainian digital infrastructure through cyber operations, ranging in type, target, and sophistication. Through some combination of Ukrainian preparedness, partner intervention, and Russian planning shortfalls, among other factors, large-scale cyber operations disrupting Ukrainian critical infrastructure, such as those seen previously in 2015 with BlackEnergy and NotPetya, did not materialize.[23] This could be because such cyber operations require significant time and resources, and similar ends can be more cheaply achieved through direct, physical means. Russian cyber operators, however, have not been idle.

16 Romain Fontugne, Ksenia Ermoshina, and Emile Aben, "The Internet in Crimea: A Case Study on Routing Interregnum," 2020 IFIP Networking Conference, Paris, France, June 22–25, 2020, https://hal.archives-ouvertes.fr/hal-03100247/document.

17 Sebastian Moss, "How Russia Took over the Internet in Crimea and Eastern Ukraine," Data Center Dynamics, January 12, 2023, https://www.datacenterdynamics.com/en/analysis/how-russia-took-over-the-internet-in-crimea-and-eastern-ukraine/; "Ukraine: Freedom on the Net 2018 Country Report," Freedom House, 2019, https://freedomhouse.org/country/ukraine/freedom-net/2018.

18 Fontugne, Ermoshina, and Aben, "The Internet in Crimea."

19 Frédérick Douzet et al., "Measuring the Fragmentation of the Internet: The Case of the Border Gateway Protocol (BGP) During the Ukrainian Crisis," 2020 12th International Conference on Cyber Conflict (CyCon), Tallinn, Estonia, May 26–29, 2020, 157-182, doi: 10.23919/CyCon49761.2020.9131726; Paul Mozur et al., "'They Are Watching': Inside Russia's Vast Surveillance State," *New York Times*, September 22, 2022, https://www.nytimes.com/interactive/2022/09/22/technology/russia-putin-surveillance-spying.html.

20 Yaropolk Brynykh and Anastasiia Lykholat, "Occupied Crimea: Victims and Oppressors," Freedom House, August 30, 2018, https://freedomhouse.org/article/occupied-crimea-victims-and-oppressors.

21 Halya Coynash, "Internet Providers Forced to Conceal Total FSB Surveillance in Occupied Crimea and Russia," *Kyiv Post*, February 2, 2018, https://www.kyivpost.com/article/opinion/op-ed/halya-coynash-internet-providers-forced-conceal-total-fsb-surveillance-occupied-crimea-russia.html.

22 "Crimea: Freedom in the World 2020 Country Report," Freedom House, https://freedomhouse.org/country/crimea/freedom-world/2020.

23 Kim Zetter, "Inside the Cunning, Unprecedented Hack of Ukraine's Power Grid," *Wired*, March 3, 2016, https://www.wired.com/2016/03/inside-cunning-unprecedented-hack-ukraines-power-grid/; Andy Greenberg, "The Untold Story of Notpetya, the Most Devastating Cyberattack in History," *Wired*, August 22, 2018, https://www.wired.com/story/notpetya-cyberattack-ukraine-russia-code-crashed-the-world/.

Preceding the physical invasion, there was a spate of activity, attributed to both Russian and Russian-aligned organizations, targeting a combination of state and private organizations.[24] From January 13 to 14, for example, hackers briefly took control of seventy Ukrainian government websites, including the Ministries of Defense and Foreign Affairs, adding threatening messages to the top of these official sites.[25] The following day, January 15, Microsoft's Threat Intelligence Center reported the discovery of wiper malware, disguised as ransomware, in dozens of Ukrainian government systems, including agencies which "provide critical executive branch or emergency response function," and an information technology firm that services those agencies.[26] A month later, on February 15, Russian hackers targeted several websites with distributed denial of service (DDoS) attacks, forcing Ukrainian defense ministry and armed forces websites, as well as those of PrivatBank and Oschadbank, offline.[27] Around the same time, according to Microsoft's special report on Ukraine, "likely" Russian actors were discovered in the networks of unidentified critical infrastructure in Odessa and Sumy.[28] The day before the invasion, cybersecurity companies ESET and Symantec reported that a new destructive wiper was spreading across Ukrainian, Latvian, and Lithuanian networks, as a second round of DDoS attacks again took down a spate of government and financial institution websites.[29] This activity centered around information—with defacements sending a clear threat to the Ukrainian government and population, DDoS attacks impairing accurate communication, and wiper malware degrading Ukrainian data—and gaining access to Ukrainian data for Russia. Although many of these operations targeted Ukrainian government networks, the attacks moved through or against privately operated infrastructure and, notably, the first public notification and detailing of several of these operations was undertaken by transnational technology companies.

After February 24, Russian cyber activity continued and the targets included a number of private information infrastructure operators. A March hack of Ukrtelecom—Ukraine's largest landline operator, which also provides internet and mobile services to civilians and the Ukrainian government and military—resulted in a collapse of the company's network to just 13 percent capacity, the most severe disruption in service the firm recorded since the invasion began.[30] Another such operation targeted Triolan—a Ukrainian telecommunications provider—on February 24 in tandem with the physical offensive and a second time on March 9. These incursions on the Triolan network took down key nodes and caused widespread service outages. Following the March 9 attack, the company was able to restore service, but these efforts were complicated by the need to physically access some

24 "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; Kyle Fendorf and Jessie Miller, "Tracking Cyber Operations and Actors in the Russia–Ukraine War," Council on Foreign Relations, March 24, 2022, https://www.cfr.org/blog/tracking-cyber-operations-and-actors-russia-ukraine-war.

25 Jakub Przetacznik and Simona Tarpova, "Russia's War on Ukraine: Timeline of Cyber-Attacks," European Parliament, June 2022, https://www.europarl.europa.eu/RegData/etudes/BRIE/2022/733549/EPRS_BRI(2022)733549_EN.pdf; Catalin Cimpanu, "Hackers Deface Ukrainian Government Websites," The Record, January 14, 2022, https://therecord.media/hackers-deface-ukrainian-government-websites/.

26 Tom Burt, "Malware Attacks Targeting Ukraine Government," Microsoft, January 15, 2022, https://blogs.microsoft.com/on-the-issues/2022/01/15/mstic-malware-cyberattacks-ukraine-government/.

27 Roman Osadchuk, *Russian Hybrid Threats Report: Evacuations Begin in Ukrainian Breakaway Regions, Atlantic Council*, February 18, 2022, https://www.atlanticcouncil.org/blogs/new-atlanticist/russian-hybrid-threats-report-evacuations-begin-in-ukrainian-breakaway-regions/#cyberattack; Sean Lyngaas and Tim Lister, "Cyberattack Hits Websites of Ukraine Defense Ministry and Armed Forces," *CNN*, February 15, 2022, https://www.cnn.com/2022/02/15/world/ukraine-cyberattack-intl/index.html.

28 Microsoft, "Special Report Ukraine."

29 "ESET Research: Ukraine Hit by Destructive Attacks Before and During the Russian Invasion with HermeticWiper and IsaacWiper," ESET, March 1, 2022, https://www.eset.com/int/about/newsroom/press-releases/research/eset-research-ukraine-hit-by-destructive-attacks-before-and-during-the-russian-invasion-with-hermet/; "Ukraine: Disk-Wiping Attacks Precede Russian Invasion," Symantec Threat Hunter Team, February 24, 2022, https://symantec-enterprise-blogs.security.com/blogs/threat-intelligence/ukraine-wiper-malware-russia; "Ukraine Computers Hit by Data-Wiping Software as Russia Launched Invasion," Reuters, February 24, 2022, https://www.reuters.com/world/europe/ukrainian-government-foreign-ministry-parliament-websites-down-2022-02-23/.

30 Britney Nguyen, "Telecom Workers in Occupied Parts of Ukraine Destroyed Software to Avoid Russian Control over Data and Communications," Business Insider, June 22, 2022, https://www.businessinsider.com/telecom-workers-ukraine-destroyed-software-avoid-russian-control-2022-6; Net Blocks (@netblocks), "Confirmed: A major internet disruption has been registered across #Ukraine on national provider #Ukrtelecom; real-time network data show connectivity collapsing ...," Twitter, March 28, 2022, 10:38 a.m., https://twitter.com/netblocks/status/1508453511176065033; Net Blocks (@netblocks), "Update: Ukraine's national internet provider Ukrtelecom has confirmed a cyberattack on its core infrastructure. Real-time network data show an ongoing and ...," Twitter, March 28, 2022 11:25 a.m., https://twitter.com/netblocks/status/1508465391244304389; Andrea Peterson, "Traffic at Major Ukrainian Internet Service Provider Ukrtelecom Disrupted," The Record, March 28, 2022, https://therecord.media/traffic-at-major-ukrainian-internet-service-provider-ukrtelecom-disrupted/; James Andrew Lewis, *Cyber War and Ukraine, Center for Strategic and International Studies*, January 10, 2023, https://www.csis.org/analysis/cyber-war-and-ukraine.

of the equipment located in active conflict zones.[31] These attacks against Ukraine-based information infrastructure companies caused service outages that were concurrent with the physical invasion and afterwards, restricted communications among Ukrainians and impeded the population's ability to respond to current and truthful information.

These types of operations, however, were not restricted to Ukraine-based information infrastructure. A significant opening salvo in Russia's invasion was a cyber operation directed against ViaSat, a private American-based satellite internet company that provides services to users throughout the world, including the Ukrainian military.[32] Instead of targeting the satellites in orbit, Russia targeted the modems in ViaSat's KA-SAT satellite broadband network that connected users with the internet.[33] Specifically, Russia exploited a "misconfiguration in a VPN [virtual private network] appliance to gain remote access to the trusted management segment of the KA-SAT network."[34] From there, the attackers were able to move laterally though the network to the segment used to manage and operate the broader system.[35] They then "overwrote key data in flash memory on the modems," making it impossible for the modems to access the broader network.[36] Overall, the effects of the hack were short-lived, with ViaSat reporting the restoration of connectivity within a few days after shipping approximately 30,000 new modems to affected customers.[37]

SentinelOne, a cybersecurity firm, identified the malware used to wipe the modems and routers of the information they needed to operate.[38] The firm assessed "with medium-confidence" that AcidRain, the malware used in the attack, had "developmental similarities" with an older malware, VPNFilter, that the Federal Bureau of Investigation and the US Department of Justice have previously linked to the Russian government.[39] The United States, United Kingdom, and European Union all subsequently attributed the ViaSat hack to Russian-state backed actors.[40]

The effectiveness of the operation is debated, although the logic of the attack is straightforward. Russia wanted to constrain, or preferably eliminate, an important channel of communication for the Ukrainian military during the initial stages of the invasion. Traditional, land-based radios, which the Ukrainian military relies on for most of their communications, only work over a limited geographic range, therefore making it more difficult to use advanced, long-range weapons systems.[41] It should be expected that landline and conventional telephony would suffer outages during the opening phases of the war and struggle to keep up with rapidly moving forces.

Initially, it was widely reported that the Russian strike on ViaSat was effective. On March 15, a senior Ukrainian cybersecurity official, Viktor Zhora, was quoted saying that the attack on ViaSat caused "a really huge loss in communications in the very beginning of the war."[42]

31 Thomas Brewster, "As Russia Invaded, Hackers Broke into A Ukrainian Internet Provider. Then Did It Again As Bombs Rained Down," Forbes, March 10, 2022, https://www.forbes.com/sites/thomasbrewster/2022/03/10/cyberattack-on-major-ukraine-internet-provider-causes-major-outages/?sh=51d16b9c6573.

32 "Global Communications: Services, Solutions and Satellite Internet," ViaSat, accessed November 14, 2022, http://data.danetsoft.com/viasat.com; Matt Burgess, "A Mysterious Satellite Hack Has Victims Far beyond Ukraine," *Wired*, March 23, 2022, https://www.wired.com/story/viasat-internet-hack-ukraine-russia/.

33 Michael Kan, "ViaSat Hack Tied to Data-Wiping Malware Designed to Shut down Modems," PCMag, March 31, 2022, https://www.pcmag.com/news/viasat-hack-tied-to-data-wiping-malware-designed-to-shut-down-modems.

34 "Ka-Sat Network Cyber Attack Overview," ViaSat, September 12, 2022, https://news.viasat.com/blog/corporate/ka-sat-network-cyber-attack-overview.

35 Lee Mathews, "ViaSat Reveals How Russian Hackers Knocked Thousands of Ukrainians Offline," Forbes, March 31, 2022, https://www.forbes.com/sites/leemathews/2022/03/31/viasat-reveals-how-russian-hackers-knocked-thousands-of-ukrainians-offline/?sh=4683638b60d6; ViaSat, "Ka-Sat Network."

36 ViaSat, "Ka-Sat Network."

37 Andrea Valentina, "Why the Viasat Hack Still Echoes," Aerospace America, November 2022, https://aerospaceamerica.aiaa.org/features/why-the-viasat-hack-still-echoes.

38 Juan Andres Guerrero-Saade and Max van Amerongen, "Acidrain: A Modem Wiper Rains down on Europe," SentinelOne, April 1, 2022, https://www.sentinelone.com/labs/acidrain-a-modem-wiper-rains-down-on-europe/.

39 Guerrero-Saade and Van Amerongen, "Acidrain."

40 Joe Uchill, "UK, US, and EU Attribute Viasat Hack Against Ukraine to Russia," SC Media, June 23, 2022, https://www.cmagazine.com/analysis/threat-intelligence/uk-us-and-eu-attribute-viasat-hack-against-ukraine-to-russia; David E. Sanger and Kate Conger, "Russia Was Behind Cyberattack in Run-Up to Ukraine War, Investigation Finds," *New York Times*, May 10, 2022, https://www.nytimes.com/2022/05/10/us/politics/russia-cyberattack-ukraine-war.html.

41 Kim Zetter, "ViaSat Hack 'Did Not' Have Huge Impact on Ukrainian Military Communications, Official Says," Zero Day, September 26, 2022, https://zetter.substack.com/p/viasat-hack-did-not-have-huge-impact; "Satellite Outage Caused 'Huge Loss in Communications' at War's Outset—Ukrainian Official," Reuters, March 15, 2022, https://www.reuters.com/world/satellite-outage-caused-huge-loss-communications-wars-outset-ukrainian-official-2022-03-15/.

42 Reuters, "Satellite Outage."

When asked follow-up questions about his quote, Zhora said at the time that he was unable to elaborate, leading journalists and industry experts to believe that the attack had impacted the Ukrainian military's ability to communicate.[43] However, several months later, on September 26, Zhora revised his initial comments, stating that the hack *would* have impacted military communications *if* satellite communications had been the Ukrainian military's principal medium of communication. However, Zhora stated that the Ukrainian military instead relies on landlines for communication, with satellites as a back-up method. He went on to say that "in the case land lines were destroyed, that could be a serious issue in the first hours of war."[44] The tension, and potential contradictions, in Zhora's comments underlines the inherent complications in analyzing cyber operations during war: long-term consequences can be difficult to infer from short-term effects, and countries seek to actively control the narratives surrounding conflict.

The effectiveness of the ViaSat hack boils down to how the Ukrainian military communicates, and how adaptable it was in the early hours of the invasion. However, it is apparent how such a hack *could* impact military effectiveness. If Russia, or any other belligerent, was able to simultaneously disrupt satellite communications while also jamming or destroying landlines, forces on the frontlines would be at best poorly connected with their superiors. In such a scenario, an army would be cut off from commanders in other locations and would not be able to report back or receive new directives; they would be stranded until communications could be restored.

The ViaSat hack had a military objective: to disrupt Ukrainian military access to satellite communications. But the effects were not limited to this objective. The operation had spillover effects that rippled across Europe. In Germany, nearly 6,000 wind turbines were taken offline, with roughly 2,000 of those turbines remaining offline for nearly a month after the initial hack due to the loss of remote connectivity.[45] In France, modems used by emergency services vehicles, including firetrucks and ambulances, were also affected.[46]

ViaSat is not a purely military target. It is a civilian firm that counts the Ukrainian military as a customer. The targeting of civilian infrastructure with dual civilian and military capacity and use has occurred throughout history and has been the center of debate in international law, especially when there are cross-border spillover effects in non-combatant countries. Both the principle of proportionality and international humanitarian law require the aggressor to target only military objects, defined as objects "whose total or partial destruction, capture or neutralization, in the circumstances ruling at the time, offers a definite military advantage" in a manner proportional to the military gain foreseen by the operation.[47] What this means in practice, however, is that the aggressor determines whether they deem a target to be a military object and a beneficial target and, therefore, what is legitimate. Konstantin Vorontsov, the Head of the Russian Delegation to the United Nations, attempted to justify Russian actions in October 2022 by saying that the use of civilian space infrastructure to aid the Ukrainian war effort may be a violation of the Outer Space Treaty, thereby rendering this infrastructure a legitimate military target.[48] Similar operations like that against ViaSat are likely to be the new norm in modern warfare. As Mauro Vignati, the adviser on new digital technologies of warfare at the Red Cross, said in November 2022, insofar as private companies own and operate the information infrastructure of the domain, including infrastructure acting as military assets, "when war start[s], those companies, they are inside the battlefield."[49]

43 ean Lyngaas, "US Satellite Operator Says Persistent Cyberattack at Beginning of Ukraine War Affected Tens of Thousands of Customers, CNN, March 30, 2022, https://www.cnn.com/2022/03/30/politics/ukraine-cyberattack-viasat-satellite/index.html.

44 Zetter, "ViaSat Hack."

45 Burgess, "A Mysterious Satellite Hack" Zetter, "ViaSat Hack"; Valentino, "Why the ViaSat Hack."

46 Jurgita Lapienytė, "ViaSat Hack Impacted French Critical Services," CyberNews, August 22, 2022, https://cybernews.com/news/viasat-hack-impacted-french-critical-services/.

47 International Committee of the Red Cross, Protocol Additional to the Geneva Conventions of 12 August 1949, and Relating to the Protection of Victims of International Armed Conflicts (Protocol I), 1125 UNTS 3 (June 8, 1977), accessed January 18, 2023, https://www.refworld.org/docid/3ae6b36b4.html; Zhanna L. Malekos Smith, "No 'Bright-Line Rule' Shines on Targeting Commercial Satellites," The Hill, November 28, 2022, https://thehill.com/opinion/cybersecurity/3747182-no-bright-line-rule-shines-on-targeting-commercial-satellites/; Anaïs Maroonian, "Proportionality in International Humanitarian Law: A Principle and a Rule," Lieber Institute West Point, October 24, 2022, https://lieber.westpoint.edu/proportionality-international-humanitarian-law-principle-rule/#:~:text=The%20rule%20of%20proportionality%20requires,destruction%20of%20a%20military%20objective; Travis Normand and Jessica Poarch, "4 Basic Principles," The Law of Armed Conflict, January 1, 2017, https://loacblog.com/loac-basics/4-basic-principles/.

48 "Statement by Deputy Head of the Russian Delegation Mr. Konstantin Vorontsov at the Thematic Discussion on Outer Space (Disarmament Aspects) in the First Committee of the 77th Session of the Unga," Permanent Mission of the Russian Federation to the United Nations, October 26, 2022, https://russiaun.ru/en/news/261022_v.

49 Mauro Vignati, "LABScon Replay: Are Digital Technologies Eroding the Principle of Distinction in War?" SentinelOne, November 16, 2022, https://www.sentinelone.com/labs/are-digital-technologies-eroding-the-principle-of-distinction-in-war/.

Physical Information Infrastructure

In February 2022, as Russian forces moved to seize airfields and key physical assets in Ukraine, they simultaneously assaulted the physical information infrastructure operating within and beneath the Ukrainian information environment. Russian forces targeted this infrastructure, largely privately operated, by taking control of assets where possible and destroying them where not, including through a series of Russian air strikes targeting Ukrainian servers, cables, and cell phone towers.[50] As of June 2022, about 15 percent of Ukrainian information infrastructure had been damaged or destroyed; by July, 12.2 percent of homes had lost access to mobile communication services, 11 percent of base stations for mobile operators were out of service, and approximately 20 percent of the country's telecommunications infrastructure was damaged or destroyed.[51] By August "the number of users connecting to the Internet in Ukraine [had] shrunk by at least 16 percent nationwide."[52]

In some areas of Ukraine, digital blackouts were enforced by Russian troops to cut the local population off from the highly contested information space. In Mariupol, the last cell tower connecting the city with the outside world was tirelessly tended by two Kyivstar engineers, who kept it alive with backup generators that they manually refilled with gasoline. Once the Russians entered the city, however, the Ukrainian soldiers who had been protecting the cell tower location left to engage with the enemy, leaving the Kyivstar engineers alone to tend to their charge. For three days the engineers withstood the bombing of the city until March 21, when Russian troops disconnected the tower and it went silent.[53]

Russian forces coerced Ukrainian occupied territories onto Russian ISPs, once again through Rostelcom's local agent Miranda Media, and onto Russian mobile service providers.[54] Information infrastructure in Ukraine is made up of overlapping networks of mobile service and ISPs, a legacy of the country's complicated post-Soviet modernization process. This complexity may have been a boon for its resilience. Russian forces, observed digital-rights researcher Samuel Woodhams, "couldn't go into one office and take down a whole region … There were hundreds of these offices and the actual hardware was quite geographically separated."[55] Across eastern Ukraine, including Kherson, Mlitopol, and Mariupol, the Russians aimed to subjugate the physical territory, constituent populations, and Ukrainian information environment. In Kherson, Russian forces entered the offices of a Ukrainian ISP and at gunpoint, forced staff to transfer control to them.[56]

Routing the internet and communications access of occupied territories through Russia meant that Moscow could suppress communications to and from these occupied areas, especially through social media and Ukranian news sites, sever access to essential services in Ukraine, and flood the populations with its own propaganda, as was proved in Crimea in 2014. Moving forward, Russia could use this dependency to "disconnect, throttle, or restrict access to the internet" in occupied territories, cutting off the occupied population from the Ukrainian government and the wider Ukrainian and international community.[57]

50 Matt Burgess, "Russia Is Taking over Ukraine's Internet," Wired, June 15, 2022, https://www.wired.com/story/ukraine-russia-internet-takeover/.

51 Nino Kuninidze et al., "Interim Assessment on Damages to Telecommunication Infrastructure and Resilience of the ICT Ecosystem in Ukraine."

52 Adam Satariano and Scott Reinhard, "How Russia Took Over Ukraine's Internet in Occupied Territories," The New York Times, August 9, 2022, https://www.nytimes.com/interactive/2022/08/09/technology/ukraine-internet-russia-censorship.html; https://time.com/6222111/ukraine-internet-russia-reclaimed-territory/

53 Thomas Brewster, "The Last Days of Mariupol's Internet," Forbes, March 31, 2022, https://www.forbes.com/sites/thomasbrewster/2022/03/31/the-last-days-of-mariupols-internet/.

54 Matt Burgess, "Russia Is Taking over Ukraine's Internet," Wired, June 15, 2022, https://www.wired.com/story/ukraine-russia-internet-takeover/; Satariano and Reinhard, "How Russia Took."

55 Vera Bergengruen, "The Battle for Control over Ukraine's Internet," Time, October 18, 2022, https://time.com/6222111/ukraine-internet-russia-reclaimed-territory/.

56 Herbert Lin, "Russian Cyber Operations in the Invasion of Ukraine," Cyber Defense Review (Fall 2022): 35, https://cyberdefensereview.army.mil/Portals/6/Documents/2022_fall/02_Lin.pdf, Herb Lin, "The Emergence of Physically Mediated Cyberattacks?," Lawfare,May 21, 2022, https://www.lawfareblog.com/emergence-physically-mediated-cyberattacks; "Invaders Use Blackmailing andIntimidation to Force Ukrainian Internet Service Providers to Connect to Russian Networks," State Service of Special Communicationsand Information Protection of Ukraine, May 13, 2022, https://cip.gov.ua/en/news/okupanti-shantazhem-i-pogrozami-zmushuyutukrayinskikh-provaideriv-pidklyuchatisya-do-rosiiskikh-merezh; Satariano and Reinhard, "How Russia Took."

57 Gian M. Volpicelli, "How Ukraine's Internet Can Fend off Russian Attacks," Wired, March 1, 2022, https://www.wired.com/story/internet-ukraine-russia-cyberattacks/; Satariano and Reinhard, "How Russia Took."

The Kremlin's primary purpose in the invasion of Ukraine was and is to remove the Ukrainian government and, likely, install a pro-Russian puppet government to bring to an end an independent Ukraine.[58] Therefore, isolating the information environment of occupied populations, in concert with anti-Ukrainian government disinformation, such as the multiple false allegations that President Zelenskyy had fled the country and abandoned the Ukrainian people,[59] were a means to sway the allegiances, or at least dilute the active resistance, of the Ukrainian people.[60] Without connectivity to alternative outlets, the occupying Russians could promote false and largely uncontested claims about the progress of the war. In early May 2022 for example, when Kherson lost connectivity for three days, the deputy of the Kherson Regional Council, Serhiy Khlan, reported that the Russians "began to spread propaganda that they were in fact winning and had captured almost all of Mykolaiv."[61]

Russia used its assault on the information environment to undermine the legitimacy of the Ukrainian government and its ability to fulfill its governmental duties to the Ukrainian people. Whether through complete connectivity blackouts or through the restrictions imposed by Russian networks, the Russians blocked any communications from the Ukrainian government to occupied populations—not least President Zelenskyy's June 13, 2022 address, intended most for those very populations, in which he promised to liberate all occupied Ukrainian land and reassured those populations that they had not been forgotten. Zelenskyy acknowledged the Russian barrier between himself and Ukrainians in occupied territories, saying, "They are trying to make people not just know nothing about Ukraine… They are trying to make them stop even thinking about returning to normal life, forcing them to reconcile."[62]

Isolating occupied populations from the Ukrainian information space is intended, in large part, said Stas Prybytko, the head of mobile broadband development within the Ukrainian Ministry of Digital Transformation, to "block them from communicating with their families in other cities and keep them from receiving truthful information."[63] Throughout 2022, so much of what the international community knew about the war came—through Twitter, TikTok, Telegram, and more—from Ukrainians themselves. From videos of the indiscriminate Russian shelling of civilian neighborhoods to recordings tracking Russian troop movements, Ukrainians used their personal devices to capture and communicate the progress of the war directly to living rooms, board rooms, and government offices around the world.[64] The power of this distributed information collection and open-source intelligence relies upon mobile and internet access. The accounts that were shared after Ukrainian towns and cities were liberated from Russian occupation lay bare just how much

58 David R. Marples, "Russia's War Goals in Ukraine," *Canadian Slavonic Papers* 64, no. 2–3 (March 2022): 207–219, https://doi.org/10.1080/00085006.2022.2107837.

59 David Klepper, "Russian Propaganda 'Outgunned' by Social Media Rebuttals," AP News, March 4, 2022, https://apnews.com/article/russia-ukraine-volodymyr-zelenskyy-kyiv-technology-misinformation-5e884b85f8dbb54d16f5f10d105fe850; Marc Champion and Daryna Krasnolutska, "Ukraine's TV Comedian President Volodymyr Zelenskyy Finds His Role as Wartime Leader," *Japan Times*, June 7, 2022, https://www.japantimes.co.jp/news/2022/02/26/world/volodymyr-zelenskyy-wartime-president/;"Российское Телевидение Сообщило Об 'Бегстве Зеленского' Из Киева, Но Умолчало Про Жертвы Среди Гражданских," Агентство, October 10, 2022, https://web.archive.org/web/20221010195154/https://www.agents.media/propaganda-obstreli/.

60 To learn more about Russian disinformation efforts against Ukraine and its allies, check out the *Russian Narratives Reports* from the Atlantic Council's Digital Forensic Research Lab: Nika Aleksejeva et al., Andy Carvin ed., "Narrative Warfare: How the Kremlin and Russian News Outlets Justified a War of Aggression against Ukraine," Atlantic Council, February 22, 2023, https://www.atlanticcouncil.org/in-depth-research-reports/report/narrative-warfare/; Roman Osadchuk et al., Andy Carvin ed., "Undermining Ukraine: How the Kremlin Employs Information Operations to Erode Global Confidence in Ukraine," Atlantic Council, February 22, 2023, https://www.atlanticcouncil.org/in-depth-research-reports/report/undermining-ukraine/.

61 Олександр Янковський, "'Бояться Спротиву'. Для Чого РФ Захоплює Мобільний Зв'язок Та Інтернет На Херсонщині?," Радіо Свобода, May 7, 2022, https://www.radiosvoboda.org/a/novyny-pryazovya-khersonshchyna-okupatsiya-rosiya-mobilnyy-zvyazok-internet/31838946.html.

62 Volodymyr Zelenskyy, "Tell People in the Occupied Territories about Ukraine, That the Ukrainian Army Will Definitely Come—Address by President Volodymyr Zelenskyy," President of Ukraine Official Website, June 13, 2022, https://www.president.gov.ua/en/news/govorit-lyudyam-na-okupovanih-teritoriyah-pro-ukrayinu-pro-t-75801.

63 Satariano and Reinhard, "How Russia Took."

64 Michael Sheldon, "Geolocating Russia's Indiscriminate Shelling of Kharkiv," DFRLab, March 1, 2022, https://medium.com/dfrlab/geolocating-russias-indiscriminate-shelling-of-kharkiv-deaccc830846; Michael Sheldon, "Kharkiv Neighborhood Experienced Ongoing Shelling Prior to February 28 Attack," DFRLab, February 28, 2022, https://medium.com/dfrlab/kharkiv-neighborhood-experienced-ongoing-shelling-prior-to-february-28-attack-f767230ad6f6; https://maphub.net/Cen4infoRes/russian-ukraine-monitor; Michael Sheldon (@Michael1Sheldon), "Damage to civilian houses in the Zalyutino neighborhood of Kharkiv. https://t.me/c/1347456995/38991 …," Twitter, February 27, 2022, 4:15 p.m., https://twitter.com/Michael1Sheldon/status/1498044130416594947; Michael Sheldon, "Missile Systems and Tanks Spotted in Russian Far East, Heading West," DFRLab, January 27, 2022, https://medium.com/dfrlab/missile-systems-and-tanks-spotted-in-russian-far-east-heading-west-6d2a4fe7717a; Jay in Kyiv (@JayinKyiv), "Not yet 24 hours after Ukraine devastated Russian positions in Kherson, a massive Russian convoy is now leaving Melitopol to replace them. This is on Alekseev …," Twitter, July 12, 2022, 7:50 a.m., https://twitter.com/JayinKyiv/status/1546824416218193921; "Eyes on Russia Map," Centre for Information Resilience, https://eyesonrussia.org/.

suffering, arrest, torture, and murder was kept hidden from international view by the purposeful isolation of the information environment and the constant surveillance of Ukrainians' personal devices.[65] The war in Ukraine has highlighted the growing impact of distributed open source intelligence during the conduct of war that is carried out by civilians in Ukraine and by the wider open source research community though various social media and messaging platforms.[66]

Russian operations against, especially transnational, digital infrastructure companies can mostly be categorized as disruption, degradation, and information gathering, which saw Russian or Russian-aligned hackers moving in and through the Ukrainian information environment. The attacks against Ukrainian physical infrastructure, however, are of a slightly different character. Invading forces employed physically mediated cyberattacks, a method defined by Herb Lin as "attacks that compromise cyber functionality through the use of or the threat of physical force" to pursue the complete destruction or seizure and occupation of this infrastructure.[67] Both ends begin with the same purpose: to create a vacuum of information between the Ukrainian government, the Ukrainian people, and the global population, effectively ending the connection between the Ukrainian information environment and the global environment. But the seizure of this infrastructure takes things a step beyond: to occupy the Ukrainian information environment and pull its infrastructure and its people into an isolated, controlled Russian information space.

65 Katerina Sergatskova, *What You Should Know About Life in the Occupied Areas in Ukraine, Wilson Center*, September 14, 2022, https://www.wilsoncenter.org/blog-post/what-you-should-know-about-life-occupied-areas-ukraine; Jonathan Landay, "Village near Kherson Rejoices at Russian Rout, Recalls Life under Occupation," Reuters, November 12, 2022, https://www.reuters.com/world/europe/village-near-kherson-rejoices-russian-rout-recalls-life-under-occupation-2022-11-11/.

66 Andrew Salerno-Garthwaite, "OSINT in Ukraine: Civilians in the Kill Chain and the Information Space," Global Defence Technology 137 (2022), https://defence.nridigital.com/global_defence_technology_oct22/osint_in_ukraine; "How Has Open-Source Intelligence Influenced the War in Ukraine?" *Economist*, August 30, 2022, https://www.economist.com/ukraine-osint-pod; Gillian Tett, "Inside Ukraine's Open-Source War," *Financial Times*, July 22, 2022, https://www.ft.com/content/297d3300-1a65-4793-982b-1ba2372241a3; Amy Zegart, "Open Secrets," *Foreign Affairs*, January 7, 2023, https://www.foreignaffairs.com/world/open-secrets-ukraine-intelligence-revolution-amy-zegart?utm_source=twitter_posts&utm_campaign=tw_daily_soc&utm_medium=social.

67 Lin, "The Emergence."

RECLAIMING THE UKRAINIAN INFORMATION ENVIRONMENT

Preparation of the Environment

The Russian assault on the Ukrainian information environment is far from unanswered. Russian efforts have been countered by the Ukrainian government in concert with allied states and with technology companies located both within and outside Ukraine. Russia's aim to pull occupied Ukrainian territory onto Russian networks to be controlled and monitored has been well understood, and Ukraine has been hardening its information infrastructure since the initial 2014 invasion. Ukraine released its Cyber Security Strategy in 2016, which laid out the government's priorities in this space, including the defense against the range of active cyber threats they face, with an emphasis on the "cyber protection of information infrastructure."[68] The government initially focused on centralizing its networks in Kyiv to make it more difficult "for Russian hackers to penetrate computers that store critical data and provide services such as pension benefits, or to use formerly government-run networks in the occupied territories to launch cyberattacks on Kyiv."[69]

As part of its digitalization and security efforts, the Ukrainian government also sought out new partners, both public and private, to build and bolster its threat detection and response capabilities. Before and since the 2022 invasion, the Ukrainian government has worked with partner governments and an array of technology companies around the world to create resilience through increased connectivity and digitalization.

Bolstering Ukrainian Connectivity

Since the 2014 invasion and annexation of Crimea, Ukraine-serving telecommunications operators have developed plans to prepare for future Russian aggression. Lifecell, the third largest Ukrainian mobile telephone operator, prepared its network for an anticipated Russian attack. The company shifted their office archives, documentation, and critical network equipment from eastern to western Ukraine, where it would be better insulated from violence, added additional network redundancy, and increased the coordination and response capabilities of their staff.[70] Similarly, Kyivstar and Vodafone Ukraine increased their network bandwidth to withstand extreme demand. In October 2021, these three companies initiated an infrastructure sharing agreement to expand LTE (Long Term Evolution) networks into rural Ukraine and, in cooperation with the Ukrainian government, expanded the 4G telecommunications network to bring "mobile network coverage to an estimated 91.6 percent of the population."[71]

The expansion and improvement of Ukrainian telecommunications continued through international partnerships as well. Datagroup, for example, announced a $20 million partnership in 2021 with Cisco, a US-based digital communications company, to modernize and expand the bandwidth of its extensive networks.[72] Since the February 2022 invasion, Cisco has also worked with the French government to provide over $5 million of secure, wireless networking equipment and software, including firewalls, for free to the Ukrainian government.[73]

68 "Cyber Security Strategy of Ukraine," Presidential Decree of Ukraine, March 15, 2016, https://ccdcoe.org/uploads/2018/10/NationalCyberSecurityStrategy_Ukraine.pdf.

69 Eric Geller, "Ukraine Prepares to Remove Data from Russia's Reach," POLITICO, February 22, 2022, https://www.politico.com/news/2022/02/22/ukraine-centralized-its-data-after-the-last-russian-invasion-now-it-may-need-to-evacuate-it-00010777.

70 Kuninidze et al., "Interim Assessment."

71 Kuninidze et al., "Interim Assessment."

72 "Datagroup to Invest $20 Million into a Large-Scale Network Modernization Project in Partnership with Cisco," Datagroup, April 8, 2021, https://www.datagroup.ua/en/novyny/datagrup-investuye-20-mln-dolariv-u-masshtabnij-proyekt-iz-m-314.

73 Lauriane Giet, "Eutech4ukraine—Cisco's Contribution to Bring Connectivity and Cybersecurity to Ukraine and Skills to Ukrainian Refugees," Futurium, June 22, 2022, https://futurium.ec.europa.eu/en/digital-compass/tech4ukraine/your-support-ukraine/ciscos-contribution-bring-connectivity-and-cybersecurity-ukraine-and-skills-ukrainian-refugees; "Communiqué de Presse Solidarité Européenne Envers l'Ukraine: Nouveau Convoi d'Équipements Informatiques," Government of France, May 25, 2022, https://minefi.hosting.augure.com/Augure_Minefi/r/ContenuEnLigne/Download?id=4FFB30F8-F59C-45A0-979E-379E3CEC18AF&filename=06%20-%20Solidarit%C3%A9%20europ%C3%A9enne%20envers%20l%E2%80%99Ukraine%20-%20nouveau%20convoi%20d%E2%80%99%C3%A9quipements%20informatiques.pdf.

This network expansion is an integral part of the Ukrainian government's digitalization plans for the country, championed by President Zelenskyy. Rather than the invasion putting an end to these efforts, Deputy Prime Minister and Minister for Digital Transformation Mykhailo Fedorov claimed that during the war "digitalization became the foundation of all our life. The economy continues to work … due to digitalization."[74] The digital provision of government services has created an alternate pathway for Ukrainians to engage in the economy and with their government. The flagship government initiative Diia, launched in February 2020, is a digital portal through which the 21.7 million Ukrainian users can access legal identification, make social services payments, register a business, and even register property damage from Russian missile strikes.[75] The Russian advance and consequent physical destruction that displaced Ukrainians means that the ability to provide government services through alternate and resilient means is more essential than ever, placing an additional premium on defending Ukrainian information infrastructure.

Backing Up a Government

As Russian forces built up along Ukraine's borders, Ukranian network centralization may have the consequences of this centralization may have increased risk, despite the country's improved defense capabilities. In preparation for the cyber and physical attacks against the country's information infrastructure, Fedorov moved to amend Ukrainian data protection laws to allow the government to store and process data in the cloud and worked closely with several technology companies, including Microsoft, Amazon Web Services, and Google, to effect the transfer of critical government data to infrastructure hosted outside the country.[76] Cloud computing describes "a collection of technologies and organizational processes which enable ubiquitous, on-demand access to a shared pool of configurable computing resources."[77] Cloud computing is dominated by the four hyperscalers—Amazon, Microsoft, Google, and Alibaba—that provide computing and storage at enterprise scale and are responsible for the operation and security of data centers all around the world, any of which could host customer data, according to local laws and regulations.[78]

According to its April 2022 Ukraine war report, Microsoft "committed at no charge a total of $107 million of technology services to support this effort" and renewed the relationship in November, promising to ensure that "government agencies, critical infrastructure and other sectors in Ukraine can continue to run their digital infrastructure and serve citizens through the Microsoft Cloud" at a value of about $100 million.[79] Amazon and Google have also committed to supporting cloud services for the Ukrainian government, for select companies, and for humanitarian organizations focused on aiding Ukraine.[80] In accordance with the Ukrainian government's concerns, Russian missile attacks targeted the Ukrainian government's main data center in Kyiv soon after the invasion, partially destroying the facility, and cyberattacks aggressively tested Ukrainian networks.[81]

Unlike other lines of aid provided by the international community to strengthen the defense of the Ukrainian information environment, cloud services are provided

74 Atlantic Council, "Ukraine's Digital Resilience: A conversation with Deputy Prime Minister of Ukraine Mykhailo Fedorov," December 2, 2022, YouTube video, https://www.youtube.com/watch?v=VI75e0QU6uE.

75 "Digital Country—Official Website of Ukraine," Ukraine Now (Government of Ukraine), accessed January 17, 2023, https://ukraine.ua/invest-trade/digitalization/; Atlantic Council, "Ukraine's Digital Resilience."

76 Brad Smith, "Extending Our Vital Technology Support for Ukraine," Microsoft, November 3, 2022, https://blogs.microsoft.com/on-the-issues/2022/11/03/our-tech-support-ukraine/; "How Amazon Is Assisting in Ukraine," Amazon, March 1, 2022, https://www.aboutamazon.com/news/community/amazons-assistance-in-ukraine; Phil Venables, "How Google Cloud Is Helping Those Affected by War in Ukraine," Google, March 3, 2022, https://cloud.google.com/blog/products/identity-security/how-google-cloud-is-helping-those-affected-by-war-in-ukraine.

77 Simon Handler, Lily Liu, and Trey Herr, *Dude, Where's My Cloud? A Guide for Wonks and Users, Atlantic Council*, July 7, 2022, https://www.atlanticcouncil.org/in-depth-research-reports/report/dude-wheres-my-cloud-a-guide-for-wonks-and-users/.

78 Handler, Liu, and Herr, "Dude, Where's My Cloud?"

79 Brad Smith, "Defending Ukraine: Early Lessons from the Cyber War," Microsoft On the Issues, November 2, 2022, https://blogs.microsoft.com/on-the-issues/2022/06/22/defending-ukraine-early-lessons-from-the-cyber-war/; Smith, "Extending Our Vital Technology."

80 Amazon, "How Amazon Is Assisting"; Sebastian Moss, "Ukraine Awards Microsoft and AWS Peace Prize for Cloud Services and Digital Support," Data Center Dynamics, January 12, 2023, https://www.datacenterdynamics.com/en/news/ukraine-awards-microsoft-and-aws-peace-prize-for-cloud-services-digital-support/; Venables, "How Google Cloud"; Kent Walker, "Helping Ukraine," Google, March 4, 2022, https://blog.google/inside-google/company-announcements/helping-ukraine/.

81 Catherine Stupp, "Ukraine Has Begun Moving Sensitive Data Outside Its Borders," Wall Street Journal, June 14, 2022, https://www.wsj.com/articles/ukraine-has-begun-moving-sensitive-data-outside-its-borders-11655199002; Atlantic Council, "Ukraine's Digital Resilience"; Smith, "Defending Ukraine."

only by the private sector.[82] While this aid has had a transformative effect on Ukrainian defense, that transformative quality has also raised concerns. Microsoft, in its special report on Ukraine, several times cites its cloud services as one of the determining factors that limited the effect of Russian cyber and kinetic attacks on Ukrainian government data centers, and details how their services, in particular, were instrumental in this defense.[83] In this same report, Microsoft claims to be most worried about those states and organizations that do not use cloud services and provides corroborating data.[84] Microsoft services, and other technology companies offering their services at a reduced rate, or for free, are acting—at least in part—out of a belief in the rightness of the Ukrainian cause. However, they are still private companies with responsibilities to shareholders or board members, and they still must seek profit. Services provided, especially establishing information infrastructure like cloud services, are likely to establish long-term business relationships with the Ukrainian government and potentially with other governments and clients, who see the effectiveness of those services illustrated through the defense of Ukraine.

Mounting an Elastic Defense

Working for Wireless

Alongside and parallel to the Ukrainian efforts to defend and reclaim occupied physical territory is the fight for Ukrainian connectivity. Ukrainian telecommunications companies have been integral to preserving connectivity to the extent possible. In March 2022, Ukrainian telecom operators Kyivstar, Vodafone Ukraine, and Lifecell made the decision to provide free national mobile roaming services across mobile provider networks, creating redundancy and resilience in the mobile network to combat frequent service outages.[85] The free mobile service provided by these companies is valued at more than UAH 980 million (USD 26.8 million).[86] In addition, Kyivstar in July 2022 committed to the allocation of UAH 300 million (about USD 8.2 million) for the modernization of Ukraine's information infrastructure in cooperation with the Ukrainian Ministry of Digital transformation.[87] The statements that accompanied the commitments from Kyivstar and Lifecell—both headquartered in Ukraine—emphasized each company's dedication to Ukrainian defense and their role in it, regardless of the short-term financial impact.[88] These are Ukrainian companies with Ukrainian infrastructure and Ukrainian customers, and their fate is tied inextricably to the outcome of this war.

As Russian forces advanced and attempted to seize control of information infrastructure, in at least one instance, Ukrainian internet and mobile service employees sabotaged their own equipment first. Facing threats of imprisonment and death from occupying Russians, employees in several Ukrtelecom facilities withstood pressure to share technical network details and instead deleted key files from the systems. According to Ukrtelecom Chief Executive Officer Yuriy Kurmaz, "The Russians tried to connect their control boards and some equipment to our networks, but they were not able to reconfigure it because we completely destroyed the software."[89] Without functional infrastructure, Russian forces struggled to pull those areas onto Russian networks.

The destruction of telecommunications infrastructure has meant that these areas and many others along the war front are, in some areas, without reliable information infrastructure, either wireless or wired. While the Ukrainian government and a bevy of local and international private sector companies battle for control of on-the-ground internet and communications infrastructure, they also pursued new pathways to connectivity.

82 Nick Beecroft, *Evaluating the International Support to Ukrainian Cyber Defense, Carnegie Endowment for International Peace*, November 3, 2022, https://carnegieendowment.org/2022/11/03/evaluating-international-support-to-ukrainian-cyber-defense-pub-88322.

83 Smith, "Defending Ukraine," 5, 6, 9.

84 Smith, "Defending Ukraine," 3, 11.

85 Thomas Brewster, "Bombs and Hackers Are Battering Ukraine's Internet Providers. 'Hidden Heroes' Risk Their Lives to Keep Their Country Online," Forbes, March 15, 2022, https://www.forbes.com/sites/thomasbrewster/2022/03/15/internet-technicians-are-the-hidden-heroes-of-the-russia-ukraine-war/?sh=be5da1428844.

86 Kuninidze et al., "Interim Assessment," 40.

87 Kuninidze et al., "Interim Assessment," 40; ""Київстар Виділяє 300 Мільйонів Гривень Для Відновлення Цифрової Інфраструктури України," Київстар, July 4, 2022, https://kyivstar.ua/uk/mm/news-and-promotions/kyyivstar-vydilyaye-300-milyoniv-gryven-dlya-vidnovlennya-cyfrovoyi.

88 Київстар, "Київстар Виділяє"; "Mobile Connection Lifecell—Lifecell Ukraine," Lifecell UA, accessed January 17, 2023, https://www.lifecell.ua/en/.

89 Ryan Gallagher, "Russia–Ukraine War: Telecom Workers Damage Own Equipment to Thwart Russia," Bloomberg, June 21, 2022), https://www.bloomberg.com/news/articles/2022-06-21/ukrainian-telecom-workers-damage-own-equipment-to-thwart-russia.

Searching for Satellite

Two days after the invasion, Deputy Prime Minister Fedorov tweeted at Elon Musk, the Chief Executive Officer of SpaceX, that "while you try to colonize Mars—Russia try [sic] to occupy Ukraine! While your rockets successfully land from space —Russian rockets attack Ukrainian civil people! We ask you to provide Ukraine with Starlink stations and to address sane Russians to stand."[90] Just another two days later, Fedorov confirmed the arrival of the first shipment of Starlink stations.[91]

Starlink, a network of low-orbit satellites working in constellations operated by SpaceX, relies on satellite receivers no larger than a backpack that are easily installed and transported. Because Russian targeting of cellular towers made communications coverage unreliable, says Fedorov, the government "made a decision to use satellite communication for such emergencies" from American companies like SpaceX.[92] Starlink has proven more resilient than any other alternative throughout the war. Due to the low orbit of Starlink satellites, they can broadcast to their receivers at relatively higher power than satellites in higher orbits. There has been little reporting on successful Russian efforts to jam Starlink transmissions, and the Starlink base stations—the physical, earthbound infrastructure that communicates directly with the satellites—are located on NATO territory, ensuring any direct attack on them would be a significant escalation in the war.[93]

Starlink has been employed across sectors almost since the war began. President Zelenskyy has used the devices himself when delivering addresses to the Ukrainian people, as well as to foreign governments and populations.[94] Fedorov has said that sustained missile strikes against energy and communication infrastructure have been effectively countered through the deployment of Starlink devices that can restore connection where it is most needed. He even called the system "an essential part of critical infrastructure."[95]

Starlink has also found direct military applications. The portability of these devices means that Ukrainian troops can often, though not always, stay connected to command elements and peer units while deployed. Ukrainian soldiers have also used internet connections to coordinate attacks on Russian targets with artillery-battery commanders.[96] The Aerorozvidka, a specialist air reconnaissance unit within the Ukrainian military that conducts hundreds of information gathering missions every day, has used Starlink devices in areas of Ukraine without functional communications infrastructure to "monitor and coordinate unmanned aerial vehicles, enabling soldiers to fire anti-tank weapons with targeted precision."[97] Reports have also suggested that a Starlink device was integrated into an unmanned surface vehicle discovered near Sevastopol, potentially used by the Ukrainian military for reconnaissance or even to carry and deliver munitions.[98] According to one Ukrainian soldier, "Starlink is our oxygen," and were it to disappear, "our army would collapse into chaos."[99]

The initial package of Starlink devices included 3,667 terminals donated by SpaceX and 1,333 terminals purchased by the United States Agency for International

90 Mykhailo Fedorov (@FedorovMykhailo), Twitter, February 26, 2022, 7:06 a.m., https://twitter.com/FedorovMykhailo/status/1497543633293266944?s=20&t=c9Uc7CDXEBr-e5-nd2hEtw.

91 Mykhailo Fedorov (@FedorovMykhailo), "Starlink — here. Thanks, @elonmusk," Twitter, February 28, 2022, 3:19 p.m., https://twitter.com/FedorovMykhailo/status/1498392515262746630?s=20&t=vtCM9UqgWRkfxfrEHzYTGg.

92 Atlantic Council, "Ukraine's Digital Resilience."

93 "How Elon Musk's Satellites Have Saved Ukraine and Changed Warfare," *Economist*, January 5, 2023, https://www.economist.com/briefing/2023/01/05/how-elon-musks-satellites-have-saved-ukraine-and-changed-warfare.

94 Alexander Freund, "Ukraine Using Starlink for Drone Strikes," Deutsche Welle, March 27, 2022, https://www.dw.com/en/ukraine-is-using-elon-musks-starlink-for-drone-strikes/a-61270528.

95 Mykhailo Fedorov (@FedorovMykhailo), "Over 100 cruise missiles attacked 🇺🇦 energy and communications infrastructure. But with Starlink we quickly restored the connection in critical areas. Starlink ...," Twitter, October 12, 2022 3:12 p.m., https://twitter.com/FedorovMykhailo/status/1580275214272802817.

96 *Economist*, "How Elon Musk's."

97 Freund, "Ukraine Using Starlink"; Nick Allen and James Titcomb, "Elon Musk's Starlink Helping Ukraine to Win the Drone War," *Telegraph*, March 18, 2022, https://www.telegraph.co.uk/world-news/2022/03/18/elon-musks-starlink-helping-ukraine-win-drone-war/; Charlie Parker, "Specialist Ukrainian Drone Unit Picks off Invading Russian Forces as They Sleep," *Times*, March 18, 2022, https://www.thetimes.co.uk/article/specialist-drone-unit-picks-off-invading-forces-as-they-sleep-zlx3dj7bb.

98 Matthew Gault, "Mysterious Sea Drone Surfaces in Crimea," *Vice*, September 26, 2022, https://www.vice.com/en/article/xgy4q7/mysterious-sea-drone-surfaces-in-crimea.

99 *Economist*, "How Elon Musk's."

Development (USAID).[100] SpaceX initially offered free Starlink service for all the devices, although the offer has already been walked back by Musk, and then reversed again. CNN obtained proof of a letter sent by Musk to the Pentagon in September 2022 stating that SpaceX would be unable to continue funding Starlink service in Ukraine. The letter requested that the Pentagon pay what would amount to "more than $120 million for the rest of the year and could cost close to $400 million for the next 12 months." It also clarified that the vast majority of the 20,000 Starlink devices sent to Ukraine were financed at least in part by outside funders like the United States, United Kingdom, and Polish governments.[101]

After the letter was sent, but before it became public, Musk got into a Twitter spat with Ukrainian diplomat Adrij Melnyk after the former wrote a tweet on October 3 proposing terms of peace between Russia and Ukraine. Musk's proposal included Ukraine renouncing its claims to Crimea and pledging to remain neutral, with the only apparent concession from Russia a promise to ensure water supply in Crimea. The plan was rejected by the public poll Musk included in the tweet, and Melnyk replied and tagged Musk, saying "Fuck off is my very diplomatic reply to you @elonmusk."[102] After CNN released the SpaceX letter to the Pentagon, Musk seemingly doubled down on his decision to reduce SpaceX funding at first. He then walked it back. He responded on October 14 to a tweet summarizing the incident, justifying possible reduced SpaceX assistance stating, "We're just following his [Melnyk's] recommendation," even though the letter was sent before the Twitter exchange. Musk then tweeted the following day, "The hell with it … even though Starlink is still losing money & other companies are getting billions of taxpayer $, we'll just keep funding Ukraine govt for free."[103] Two days later, in response to a Politico tweet reporting that the Pentagon was considering covering the Starlink service costs, Musk stated that "SpaceX has already withdrawn its request for funding."[104] Musk's characterization of SpaceX's contribution to the war effort has sparked confusion and reprimand, with his public remarks often implying that his company is entirely footing the bill when in fact, tens of millions of dollars' worth of terminals and service are being covered by several governments every month.

The Starlink saga, however, was not over yet. Several weeks later in late October, 1,300 Starlink terminals in Ukraine, purchased in March 2020 by a British company for use in Ukrainian combat-related operations, were disconnected, allegedly due to lack of funding, causing a communications outage for the Ukrainian military.[105] Although operation was restored, the entire narrative eroded confidence in SpaceX as a guarantor of flexible connectivity in Ukraine. In November 2022, Federov noted that while Ukraine has no intention of breaking off its relationship with Starlink, the government is exploring working with other satellite communications operators.[106] Starlink is not the only satellite communications network of its kind, but its competitors have not yet reached the same level of operation. Satellite communications company OneWeb, based in London with ties to the British military, is just now launching its satellite constellation, after the Russian invasion of Ukraine required the company to change its launch partner from Roscosmos to SpaceX.[107] The US Space Development Agency, within the United States Space Force, will launch the first low earth orbit satellites of the new National Defense Space Architecture in March 2023. Other more traditional satellite companies cannot provide the same flexibility as Starlink's small, transportable receivers.

100 Akash Sriram, "SpaceX, USAID Deliver 5,000 Satellite Internet Terminals to Ukraine Akash Sriram," Reuters, April 6, 2022, https://www.reuters.com/technology/spacex-usaid-deliver-5000-satellite-internet-terminals-ukraine-2022-04-06/.

101 Alex Marquardt, "Exclusive: Musk's Spacex Says It Can No Longer Pay for Critical Satellite Services in Ukraine, Asks Pentagon to Pick up the Tab," CNN, October 14, 2022, https://www.cnn.com/2022/10/13/politics/elon-musk-spacex-starlink-ukraine.

102 Elon Musk (@elonmusk), "Ukraine-Russia Peace: - Redo elections of annexed regions under UN supervision. Russia leaves if that is will of the people. - Crimea formally part of Russia, as it has been since 1783 (until …" Twitter, October 3, 2022 12:15 p.m., https://twitter.com/elonmusk/status/1576969255031296000; Andrij Melnyk (@MelnykAndrij), Twitter, October 3, 2022, 12:46 p.m., https://twitter.com/MelnykAndrij/status/1576977000178208768.

103 Elon Musk (@elonmusk), Twitter, October 14, 2022, 3:14 a.m., https://twitter.com/elonmusk/status/1580819437824839681; Elon Musk (@elonmusk), Twitter, October 15, 2022, 2:06 p.m., https://twitter.com/elonmusk/status/1581345747777179651.

104 Elon Musk (@elonmusk), Twitter, October 17, 2022, 3:52 p.m., https://twitter.com/elonmusk/status/1582097354576265217; Sawyer Merrit (@SawyerMerritt), "BREAKING: The Pentagon is considering paying for @SpaceX 's Starlink satellite network — which has been a lifeline for Ukraine — from a fund that has been used …," Twitter, October 17, 2022, 3:09 p.m., https://twitter.com/SawyerMerritt/status/1582086349305262080.

105 Alex Marquardt and Sean Lyngaas, "Ukraine Suffered a Comms Outage When 1,300 SpaceX Satellite Units Went Offline over Funding Issues" CNN, November 7, 2022, https://www.cnn.com/2022/11/04/politics/spacex-ukraine-elon-musk-starlink-internet-outage/; Iyengar, "Why Ukraine Is Stuck."

106 Ryan Browne, "Ukraine Government Is Seeking Alternatives to Elon Musk's Starlink, Vice PM Says," CNBC, November 3, 2022, https://www.cnbc.com/2022/11/03/ukraine-government-seeking-alternatives-to-elon-musks-starlink.html.

107 William Harwood, "SpaceX Launches 40 OneWeb Broadband Satellites, Lighting up Overnight Sky," CBS News, January 10, 2023, https://www.cbsnews.com/news/spacex-launches-40-oneweb-broadband-satellites-in-overnight-spectacle/.

With the market effectively cornered for the moment, SpaceX can dictate the terms, including the physical bounds, of Starlink's operations, thereby wielding immense influence on the battlefield. Starlink devices used by advancing Ukrainian forces near the front, for example, have reported inconsistent reliability.[108] Indeed CNN reported on February 9th that this bounding was a deliberate attempt to separate the devices from direct military use, as SpaceX President Gwen Shotwell explained "our intent was never to have them use it for offensive purposes."[109] The bounding decision, similar to the rationale behind the company's decision to refuse to activate Starlink service in Crimea, was likely made to contain escalation, especially escalation by means of SpaceX devices.[110]

SpaceX is not the only satellite company making decisions to bound the area of operation of their products to avoid playing—or being perceived to play—a role in potential escalation. On March 16, 2022, Minister Fedorov tweeted at DJI, a Chinese drone producer, "@DJIGlobal are you sure you want to be a partner in these murders? Block your products that are helping russia to kill the Ukrainians!"[111] DJI responded directly to the tweet the same day, saying "If the Ukrainian government formally requests that DJI set up geofencing throughout Ukraine, we will arrange it," but pointed out that such geofencing would inhibit all users of their product in Ukraine, not just Russians.[112]

While Russia continues to bombard the Ukrainian electrical grid, Starlink terminals have grown more expensive for new Ukrainian consumers, increasing from $385 earlier this year to $700, although it is unclear if this price increase also affected government purchasers.[113] According to Andrew Cavalier, a technology industry analyst with ABI research, the indispensability of the devices gives "Musk and Starlink a major head start [against its competitors] that its use in the Russia–Ukraine war will only consolidate."[114] Indeed, the valuation of SpaceX was $127 million in May 2022, and the company raised $2 billion in the first seven months of 2022.[115] For SpaceX, the war in Ukraine has been an impressive showcase of Starlink's capabilities and has proven the worth of its services to future customers. The company recently launched a new initiative, Starshield, intended to leverage "SpaceX's Starlink technology and launch capability to support national security efforts. While Starlink is designed for consumer and commercial use, Starshield is designed for government use."[116] It is clear that SpaceX intends to capitalize on the very public success of its Starlink network in Ukraine.

108 Marquardt and Lyngaas, "Ukraine Suffered"; Mehul Srivastava et al., "Ukrainian Forces Report Starlink Outages During Push Against Russia," *Financial Times*, October 7, 2022, https://www.ft.com/content/9a7b922b-2435-4ac7-acdb-0ec9a6dc8397.

109 Alex Marquardt and Kristin Fisher, "SpaceX admits blocking Ukrainian troops from using satellite technology," CNN, February 9, https://www.cnn.com/2023/02/09/politics/spacex-ukrainian-troops-satellite-technology/index.html.

110 Charles R. Davis, "Elon Musk Blocked Ukraine from Using Starlink in Crimea over Concern that Putin Could Use Nuclear Weapons, Political Analyst Says," Business Insider, October 11, 2022, https://www.businessinsider.com/elon-musk-blocks-starlink-in-crimea-amid-nuclear-fears-report-2022-10; Elon Musk (@elonmusk), Twitter, February 12, 2022, 4:00 p.m., https://twitter.com/elonmusk/status/1624876021433368578.

111 Mykhailo Fedorov (@FedorovMykhailo), "In 21 days of the war, russian troops has already killed 100 Ukrainian children. they are using DJI products in order to navigate their missile. @DJIGlobal are you sure you want to be a ...," Twitter, March 16, 2022, 8:14 a.m., https://twitter.com/fedorovmykhailo/status/1504068644195733504; Cat Zakrzewski, "4,000 Letters and Four Hours of Sleep: Ukrainian Leader Wages Digital War," *Washington Post*, March 30, 2022, https://www.washingtonpost.com/technology/2022/03/30/mykhailo-fedorov-ukraine-digital-front/.

112 DJI Global (@DJIGlobal), "Dear Vice Prime Minister Federov: All DJI products are designed for civilian use and do not meet military specifications. The visibility given by AeroScope and further Remote ID ...," Twitter, March 16, 2022, 5:42 p.m., https://twitter.com/DJIGlobal/status/1504206884240183297.

113 Mehul Srivastava and Roman Olearchyk, "Starlink Prices in Ukraine Nearly Double as Mobile Networks Falter," *Financial Times*, November 29, 2022, https://www.ft.com/content/f69b75cf-c36a-4ab3-9eb7-ad0aa00d230c.

114 Iyengar, "Why Ukraine Is Stuck."

115 Michael Sheetz, "SpaceX Raises Another $250 Million in Equity, Lifts Total to $2 Billion in 2022," CNBC, August 5, 2022, https://www.cnbc.com/2022/08/05/elon-musks-spacex-raises-250-million-in-equity.html.

116 "Starshield," SpaceX, accessed January 17, 2023, https://www.spacex.com/starshield/; Micah Maidenberg and Drew FitzGerald, "Elon Musk's Spacex Courts Military with New Starshield Project," *Wall Street Journal*, December 8, 2022), https://www.wsj.com/articles/elon-musks-spacex-courts-military-with-new-starshield-project-11670511020.

Reclaiming Territory

The Russian assault is not over, but Ukraine has reclaimed "54 percent of the land Russia has captured since the beginning of the war" and the front line has remained relatively stable since November 2022.[117] Videos and reports from reclaimed territory show the exultation of the liberated population. As Ukrainian military forces reclaim formerly occupied areas, the parallel reclamation of the information environment, by or with Ukrainian and transnational information infrastructure operators, can begin.

In newly liberated areas, Starlink terminals are often the first tool for establishing connectivity. In Kherson, the first regional capital that fell to the Russian invasion and reclaimed by Ukrainian troops on November 11, 2022, residents lined up in public spaces to connect to the internet through Starlink.[118] The Ministry of Digital Transformation provided Starlink devices to the largest service providers, Vodaphone and Kyivstar, to facilitate communication while their engineers repaired the necessary infrastructure for reestablishing mobile and internet service.[119] A week after Kherson was recaptured, five Kyivstar base stations were made operational and Vodaphone reestablished coverage over most of the city.[120]

Due to the importance of reclaiming the information environment, operators are working just behind Ukrainian soldiers to reconnect populations in reclaimed territories to the Ukrainian and global information environment as quickly as possible, which means working in very dangerous conditions. In the Sumy region in early October 2022, a Ukrtelecom vehicle pulling up to a television tower drove over a land mine, injuring three of the passengers and killing the driver.[121] Stanislav Prybytko, the head of the mobile broadband department in the Ukrainian Ministry of Digital Transformation, says "It's still very dangerous to do this work, but we can't wait to do this, because there are a lot of citizens in liberated villages who urgently need to connect."[122] Prybytko and his eleven-person team have been central to the Ukrainian effort to stitch Ukrainian connectivity back together. The team works across a public-private collaborative, coordinating with various government officials and mobile service providers to repair critical nodes in the network and to reestablish communications and connectivity.[123] According to Ukrainian government figures, 80 percent of liberated settlements have partially restored internet connection, and more than 1,400 base stations have been rebuilt by Ukrainian mobile operators since April 2022.[124]

117 "Maps: Tracking the Russian Invasion of Ukraine," *New York Times*, February 14, 2022, https://www.nytimes.com/interactive/2022/world/europe/ukraine-maps.html#:~:text=Ukraine%20has%20reclaimed%2054%20percent,for%20the%20Study%20of%20War; Júlia Ledur, Laris Karklis, Ruby Mellen, Chris Alcantara, Aaron Steckelberg and Lauren Tierney, "Follow the 600-mile front line between Ukrainian and Russian forces," The Washington Post, February 21, 2023, https://www.washingtonpost.com/world/interactive/2023/russia-ukraine-front-line-map/.

118 Jimmy Rushton (@JimmySecUK), "Ukrainian soldiers deploying a Starlink satellite internet system in liberated Kherson, allowing local residents to communicate with their relatives in other areas of Ukraine," Twitter, November 12, 2022, 8:07 a.m., https://twitter.com/JimmySecUK/status/1591417328134402050; José Andrés (@chefjoseandres), "@elonmusk While I don't agree with you about giving voice to people that brings the worst out of all of us, thanks for @SpaceXStarlink in Kherson, a city with no electricity, or in a train from ...," Twitter, November 20, 2022, 1:58 a.m., https://twitter.com/chefjoseandres/status/1594223613795762176.

119 Mykhailo Fedorov (@FedorovMykhailo), "Every front makes its contribution to the upcoming victory. These are Anatoliy, Viktor, Ivan and Andrii from @Vodafone_UA team, who work daily to restore mobile and Internet communications ...," Twitter, April 25, 2022, 1:13 p.m., https://twitter.com/FedorovMykhailo/status/1518639261624455168; Mykhailo Fedorov (@FedorovMykhailo), "Can you see a Starlink? But it's here. While providers are repairing cable damages, Gostomel's humanitarian headquarter works via the Starlink. Thanks to @SpaceX ...," Twitter, May 8, 2022, 9:48 a.m., https://twitter.com/FedorovMykhailo/status/1523298788794052615.

120 Thomas Brewster, "Ukraine's Engineers Dodged Russian Mines to Get Kherson Back Online–with a Little Help from Elon Musk's Satellites," Forbes, November 18, 2022, https://www.forbes.com/sites/thomasbrewster/2022/11/18/ukraine-gets-kherson-online-after-russian-retreat-with-elon-musk-starlink-help/?sh=186e24b0ef1e.

121 Mark Didenko, ed., "Ukrtelecom Car Hits Landmine in Sumy Region, One Dead, Three Injured," Yahoo!, October 2, 2022, https://www.yahoo.com/video/ukrtelecom-car-hits-landmine-sumy-104300649.html.

122 Vera Bergengruen, "The Battle for Control over Ukraine's Internet," Time, October 18, 2022, https://time.com/6222111/ukraine-internet-russia-reclaimed-territory/.

123 Bergengruen, "The Battle for Control over Ukraine's Internet."

124 Atlantic Council, "Ukraine's Digital Resilience: A conversation with Deputy Prime Minister of Ukraine Mykhailo Fedorov," December 2, 2022, YouTube video, https://www.youtube.com/watch?v=Vl75e0QU6uE; "Keeping connected: connectivity resilience in Ukraine," EU4Digital, February 13, 2022, https://eufordigital.eu/keeping-connected-connectivity-resilience-in-ukraine/.

KEY TAKEAWAYS

The information environment is a key domain through which this war is being contested. The Russian government has demonstrated for over a decade the importance it places on control of the information environment, both domestically and as part of campaigns to expand the Russian sphere of influence abroad. Yet, despite this Russian focus, the Ukrainian government has demonstrated incredible resilience against physical assaults, cyberattacks, and disinformation campaigns against and within the Ukrainian information environment and has committed to further interlacing government services and digital platforms.

The centrality of this environment to the conduct of this war means that private actors are necessarily enmeshed in the conflict. As providers of products and services used for Ukrainian defense, these companies are an important part of the buttressing structure of that defense. The centrality of private companies in the conduct of the war in Ukraine brings to light new and increasingly important questions about what it means for companies to act as information infrastructure during wartime, including:

1. What is the complete incentive structure behind a company's decision to provide products or services to a state at war?

2. How dependent are states on the privately held portions of the information environment, including infrastructure, tools, knowledge, data, skills, and more, for their own national security and defense?

3. How can the public and private sectors work together better as partners to understand and prepare these areas of reliance during peace and across the continuum of conflict in a sustained, rather than ad hoc, nature?

Incentives

The war in Ukraine spurred an exceptional degree of cooperation and aid from private companies within Ukraine and from around the globe. Much of public messaging around the private sector's assistance of Ukrainian defense centers around the conviction of company leadership and staff that they were compelled by a responsibility to act. This is certainly one factor in their decision. But the depth of private actor involvement in this conflict demands a more nuanced understanding of the full picture of incentives and disincentives that drive a company's decision to enter into new, or expand upon existing, business relationships with and in a country at war. What risks, for example, do companies undertake in a war in which Russia has already demonstrated its conviction that private companies are viable military targets? The ViaSat hack was a reminder of the uncertainty that surrounds the designation of dual-use technology, and the impact that such designations have in practice. What role did public recognition play in companies' decisions to provide products and services, and how might this recognition influence future earnings potential? For example, while their remarks differed in tone, both Elon Musk on Twitter and Microsoft in its special report on Ukraine publicly claimed partial credit for the defense of Ukraine.

As the war continues into its second year, these questions are important to maintaining Ukraine's cooperation with these entities. With a better understanding of existing and potential incentives, the companies, the United States, and its allies can make the decision to responsibly aid Ukraine much easier.

Dependencies

Private companies play an important role in armed conflict, operating much of the infrastructure that supports the information environment through which both state and non-state actors compete for control. The war in Ukraine has illustrated the willingness of private actors, from Ukrainian telecommunications companies to transnational cloud and satellite companies, to participate as partners in the defense of Ukraine. State dependence on privately held physical infrastructure is not unique to the information environment, but state dependence on infrastructure that is headquartered and operated extraterritorially is a particular feature.

Prior to and throughout the war, the Ukrainian government has coordinated successfully with local telecommunication companies to expand, preserve, and restore mobile, radio, and internet connectivity to its population. This connectivity preserved what Russia was attempting to dismantle—a free and open Ukrainian information environment through which the Ukrainian government and population can communicate and coordinate. The Ukrainian government has relied on these companies to provide service and connectivity, working alongside

them before and during the war to improve infrastructure and to communicate priorities. These companies are truly engaging as partners in Ukrainian defense, especially because this information infrastructure is not just a medium through which Russia launches attacks but an environment that Russia is attempting to seize control of. This dependence has not been unidirectional—the companies themselves are inextricably linked to this conflict through their infrastructure, employees, and customers in Ukraine. Each is dependent to some degree on the other and during times of crisis, their incentives create a dynamic of mutual need.

The Ukrainian government has also relied on a variety of transnational companies though the provision of technology products or services and information infrastructure. As examined in this report, two areas where the involvement of these companies has been especially impactful are cloud services and satellite internet services. Cloud services have preserved data integrity and security by moving information to data centers distributed around the world, outside of Ukrainian territory and under the cyber-protection of those cloud service companies. Satellite services have enabled flexible and resilient connectivity, once again located and run primarily outside of Ukraine. These companies can provide essential services within the information environment and the physical environment of Ukraine, but are not fundamentally reliant on the integrity of the country. This dynamic is heightened by the fact that cloud service providers like Microsoft, Amazon Web Services, Google, and satellite internet service providers like Space X's Starlink are operating within a market with global reach and very few competitors. While these companies and others have made the laudable decision to contribute to Ukrainian defense, the fact is that had they not, there are only a few, if any, other companies with comparable capabilities and infrastructure at scale. Additionally, there's very little Ukraine or even the US government could have done to directly provide the same capabilities and infrastructure.

Coordination

Built into the discussions around dependency and incentives is the need for government and the private companies who own and operate information infrastructure to coordinate with each other from a more extensive foundation. While coordination with Ukrainian companies and some transnational companies emerged from sustained effort, many instances of private sector involvement were forged on an ad hoc basis and therefore could not be planned on in advance. The ad hoc approach can produce rapid results, as seen by Minister Fedorov's tweet at Elon Musk and receipt of Starlink devices just days later. While this approach has been wielded by the Ukrainian government, and the Ministry for Digital Transformation in particular, to great effect, this very same example illustrates the complexity of transforming ad hoc aid into sustainable partnerships. Sustainability is especially important when states are facing threats outside of open war, across the continuum of insecurity and conflict where many of these capabilities and infrastructures will continue to be relied upon. Security and defense in the information environment requires states to work in coordination with a diverse range of local and transnational private actors.

Recommendations

Key recommendations from this paper ask the US government, in coordination with the Ukrainian government, to better understand the incentives that surround private sector involvement, to delineate states' dependency on private information infrastructure, and to improve long-term public-private coordination through three pathways:

- Define support parameters. Clarify how private technology companies can and should provide support
- Track support. Create a living database to track the patterns of technological support to Ukraine from US private companies
- Facilitate support requests. Add to the resilience of the Ukrainian information environment by facilitating US private support.

Define support parameters

Private information infrastructure companies will continue to play a key role in this war. However, there are a number of unresolved questions regarding the decisions these companies are making about if, and how, to provide support to the Ukrainian government to sustain its defense. A significant barrier may be the lack of clarity about the risks of partnership in wartime, which may disincentivize action or may alter existing partnerships. Recent SpaceX statements surrounding the bounding of Starlink use is an example, at least in part, of just such a rist calculous in action. The US government and its allies should release a public directive clarifying how companies can ensure that their involvement is in line with US and international law—especially for dual-use technologies.

Reaffirming, with consistent guidelines, how the United States defines civilian participation in times of war will be crucial for ensuring that such actions do not unintentionally legitimize private entities as belligerents and legitimate targets in wartime. At the direction of the National Security Advisor, the US Attorney General and Secretary of State, working through the Office of the Legal Advisor at the State Department, should issue public guidance on how US companies can provide essential support to Ukraine while avoiding the designation of legitimate military target or combatant under the best available interpretation of prevailing law.

Track support

While a large amount of support for Ukraine has been given directly by, or coordinated through governments, many private companies have started providing technological support directly to the Ukrainian government. Some private companies, especially those with offices or customers in Ukraine, got in touch directly with, or were contacted by, various Ukrainian government offices, often with specific requests depending on the company's products and services.[125]

This type of support has absolutely been effective to a degree, thanks in large part to philanthropic and private efforts to facilitate these connections.[126] However, the US government does not have a full and complete picture of this assistance, which limits the ability of US policymakers to track the implications of changing types of support or the nature of the conflict. Policymakers should have access to not only what kind of support is being provided by private US companies, but also the projected period of involvement, what types of support are being requested and denied by companies (in which case, where the US government may be able to act as an alternative provider), and what types of support are being supplied by private sector actors without a significant government equity or involvement. A more fulsome mapping of this assistance and its dependency structure would make it possible for policymakers and others to assess its impact and effectiveness. This data, were it or some version of it publicly available, would also help private companies providing the support to better understand how their contributions fit within the wider context of US assistance and to communicate the effect their products or services are having to stakeholders and shareholders. Such information may play a role in a company's decision to partner or abstain in the future.

The US government should create a collaborative task force to track US-based private sector support to Ukraine. Because of the wide equities across the US government in this area, this team should be led by the State Department's Bureau of Cyberspace and Digital Policy and include representatives from USAID, the Department of Defense's Cyber Policy Office, the National Security Agency's Collaboration Center, and the Cybersecurity and Infrastructure Security's Joint Cyber Defense Collaborative. This task force should initially focus on creating a picture of public-private support to Ukraine from entities within the United States, but its remit could extend to work with allies and partners, creating a fulsome picture of international public-private support.

Facilitate support requests

Tracking the technical support that is requested, promised, and delivered to the Ukrainian government is an important first step toward gaining a better understanding of the evolving shape of the critical role that the private sector is increasingly playing in conflict. But closer tracking, perhaps by an associated body, could go further by acting as a process facilitator. Government offices and agencies have long been facilitators of private aid, but now states are increasingly able to interact with, and request support from, private companies directly, especially for smaller quantities or more specific products and services. While this pathway can be more direct and efficient, it also requires a near constant churn of request, provision, and renewal actions from private companies and Ukrainian government officials.

Private organizations have stepped into this breach, including the Cyber Defense Assistance Collaboration (CDAC), founded by Greg Rattray and Matthew Murray, now a part of the US-based non-profit CRDF Global. CDAC works with a number of US private technology companies, as well as the National Security and Defense Council of Ukraine and the Ukrainian think tank Global Cyber Cooperative Center, to match the specific needs

125 Greg Rattray, Geoff Brown, and Robert Taj Moore, "The Cyber Defense Assistance Imperative Lessons from Ukraine," The Aspen Institute, February 16, 2023, https://www.aspeninstitute.org/wp-content/uploads/2023/02/Aspen-Digital_The-Cyber-Defense-Assistance-Imperative-Lessons-from-Ukraine.pdf, 8.

126 One such example, reviewed by the authors and led by a former Atlantic Council non-resident senior fellow Greg Rattray, is the Cyber Defense Assistance Collaboration.

of Ukrainian government and state-owned enterprises with needed products and services offered by companies working in coordination.[127]

The growth and reach of this effort demonstrate the potential impact that a government-housed, or even a government-sponsored mechanism, could have in increasing the capacity to facilitate requests from the Ukrainian government, decreasing the number of bureaucratic steps required by Ukrainian government officials while increasing the amount and quality of support they receive. In addition, government facilitation would ease progress toward the previously stated recommendations by building in clarity around what kind of support can be provided and putting facilitation and support tracking within a single process. As discussed above, this facilitation should start with a focus on US public-private support, but can grow to work alongside similar allied efforts. This could include, for example, coordination with the United Kingdom's Foreign, Commonwealth and Development Office (FCDO) program, which "enables Ukrainian agencies to access the services of commercial cybersecurity companies."[128] Crucially, this task force, helmed by the State Department's Bureau of Cyberspace and Digital Policy, would act as a facilitator, not as a restricting body. Its mission in this task would be to make connections and provide information.

In line with tracking, US government facilitation would enable government entities to communicate where assistance can be most useful, such as shoring up key vulnerabilities or ensuring that essential defense activities are not dependent on a single private sector entity, and ideally, avoiding dependency on a single source of private sector assistance. A company's financial situation or philanthropic priorities are always subject to change, and the US government should be aware of such risks and create resilience through redundancy.

Central to this resilience will be the provision of support to bolster key nodes in the Ukrainian telecommunications infrastructure network against not just cyber attacks but also against physical assault, including things like firewalls, mine clearing equipment, and power generators. Aiding the Ukrainian government in the search for another reliable partner for satellite communication devices that offer similar flexibility as Starlink is also necessary, and a representative from the Pentagon has confirmed that such a process is underway, following Musk's various and contradictory statements regarding the future of SpaceX's aid to Ukraine back in October.[129] Regardless, the entire SpaceX experience illustrates the need to address single dependencies in advance whenever possible.

A roadblock to ensuring assistance redundancy is the financial ability of companies to provide products and services to the Ukrainian government without charge or to the degree necessary. While the US government does provide funding for private technological assistance (as in the Starlink example), creating a pool of funding that is tied to the aforementioned task force and overseen by the State Department's Bureau of Cyberspace and Digital Policy, would enable increased flexibility for companies to cover areas of single dependence, even in instances that would require piecemeal rather than one-to-one redundancy. As previously discussed, many companies are providing support out of a belief that it is the right thing to do, both for their customers and as members of a global society. However, depending on whether that support is paid or provided for free, or publicly or privately given, a mechanism that provides government clarity on support provision, tracks the landscape of US private support to Ukraine, and facilitates support requests would make it easier for companies to make the decision to start or continue to provide support when weighed against the costs and potential risks of offering assistance.

127 CRDF Global, "CRDF Global becomes Platform for Cyber Defense Assistance Collaborative (CDAC) for Ukraine," News 19, November 14, 2022, https://whnt.com/business/press-releases/cision/20221114DC34776/crdf-global-becomes-platform-for-cyber-defense-assistance-collaborative-cdac-for-ukraine/; Dina Temple-Raston, "EXCLUSIVE: Rounding Up a Cyber Posse for Ukraine," The Record, November 18, 2022, https://therecord.media/exclusive-rounding-up-a-cyber-posse-for-ukraine/; Rattray, Brown, and Moore, "The Cyber Defense Assistance Imperative Lessons from Ukraine."

128 Beecroft, *Evaluating the International Support*.

129 Lee Hudson, "'There's Not Just SpaceX': Pentagon Looks Beyond Starlink after Musk Says He May End Services in Ukraine," POLITICO, October 14, 2022, https://www.politico.com/news/2022/10/14/starlink-ukraine-elon-musk-pentagon-00061896.

Looking Forward and Inward

The questions that have emerged from Ukraine's experience of defense in and through the information environment are not limited to this context. Private companies have a role in armed conflict and that role seems likely to grow, along with the scale, complexity, and criticality of the information infrastructures they own and operate. Companies will, in some capacity, be participants in the battlespace. This is being demonstrated in real time, exposing gaps that the United States and its allies and partners must address in advance of future conflicts.

Russia's war on Ukraine has created an environment in which both public and private assistance in support of Ukrainian information infrastructure is motivated by a common aversion toward Russian aggression, as well as a commitment to the stability and protection of the Ukrainian government and people. This war is not over and despite any hopes to the contrary, similar aggressions will occur in new contexts, and with new actors in the future. It is crucial that in conjunction with examining and mitigating the risks related to the involvement of private technology companies in the war in Ukraine, the US government also examines these questions regarding its own national security and defense.

The information environment is increasingly central to not just warfighting but also to the practice of governance and the daily life of populations around the world. Governments and populations live in part within that environment and therefore atop infrastructure that is owned and operated by the private sector. As adversaries seek to reshape the information environment to their own advantage, US and allied public and private sectors must confront the challenges of their existing interdependence. This includes defining in what form national security and defense plans in and through the information environment are dependent upon private companies, developing a better understanding of the differing incentive structures that guide private sector decision-making, and working in coordination with private companies to create a more resilient information infrastructure network through redundancy and diversification. It is difficult to know what forms future conflict and future adversaries will take, or the incentives that may exist for companies in those new contexts, but by better understanding the key role that private information and technology companies already play in this domain, the United States and allies can better prepare for future threats.

ABOUT THE AUTHORS

Emma Schroeder is an Associate Director with the Atlantic Council's Cyber Statecraft Initiative, within the Digital Forensic Research Lab, and leads the team's work studying conflict in and through cyberspace. Her focus in this role is on developing statecraft and strategy for cyberspace that is useful for both policymakers and practitioners. Schroeder holds an MA in History of War from King's College London's War Studies Department and also attained her BA in International Relations & History from the George Washington University's Elliott School of International Affairs.

Sean Dack was a Young Global Professional with the Cyber Statecraft Initiative during the fall of 2022. He is now a Researcher at the NATO Parliamentary Assembly, where he focuses on the long-term strategic and economic implications of Russia's invasion of Ukraine. Dack graduated from Johns Hopkins School of Advanced International Studies in December 2022 with his MA in Strategic Studies and International Economics.

ACKNOWLEDGEMENTS

Authors thank Justin Sherman, Gregory Rattray, and Gavin Wilde for their comments on earlier drafts of this document, and Trey Herr and the Cyber Statecraft team for their support. The authors also thank all the participants, who shall remain anonymous, in multiple Chatham House Rule discussions and one-on-one conversations about the issues.

Atlantic Council

Board of Directors

CHAIRMAN
*John F.W. Rogers

EXECUTIVE CHAIRMAN EMERITUS
*James L. Jones

PRESIDENT AND CEO
*Frederick Kempe

EXECUTIVE VICE CHAIRS
*Adrienne Arsht
*Stephen J. Hadley

VICE CHAIRS
*Robert J. Abernethy
*C. Boyden Gray
*Alexander V. Mirtchev

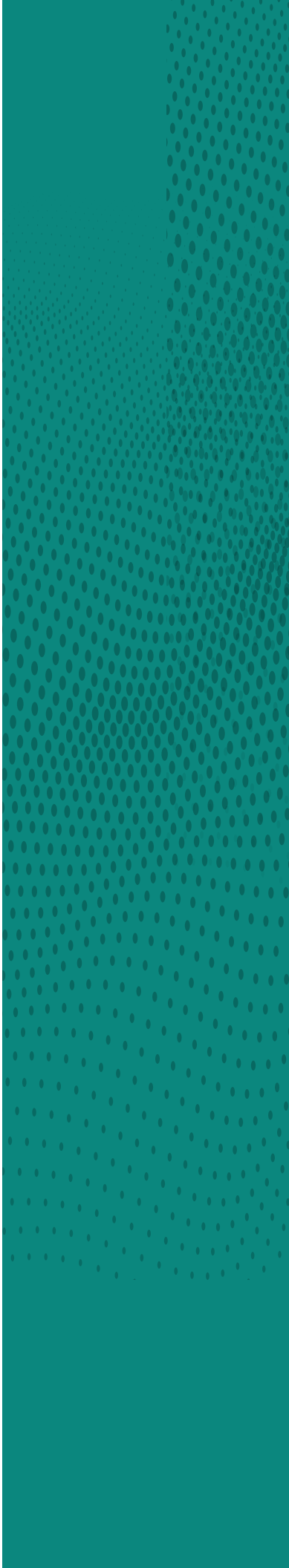
TREASURER
*George Lund

DIRECTORS
Todd Achilles
Timothy D. Adams
*Michael Andersson
David D. Aufhauser
Barbara Barrett
Colleen Bell
Stephen Biegun
Linden P. Blue
Adam Boehler
John Bonsell
Philip M. Breedlove
Myron Brilliant
*Esther Brimmer
Richard R. Burt
*Teresa Carlson
*James E. Cartwright
John E. Chapoton
Ahmed Charai
Melanie Chen
Michael Chertoff
*George Chopivsky
Wesley K. Clark
*Helima Croft
*Ankit N. Desai
Dario Deste
*Paula J. Dobriansky
Joseph F. Dunford, Jr.
Richard Edelman
Thomas J. Egan, Jr.
Stuart E. Eizenstat
Mark T. Esper
*Michael Fisch
Alan H. Fleischmann
Jendayi E. Frazer
Meg Gentle
Thomas H. Glocer
John B. Goodman
*Sherri W. Goodman
Jarosław Grzesiak
Murathan Günal
Frank Haun
Michael V. Hayden
Tim Holt
*Karl V. Hopkins
Kay Bailey Hutchison
Ian Ihnatowycz
Mark Isakowitz
Wolfgang F. Ischinger
Deborah Lee James
*Joia M. Johnson
*Safi Kalo
Andre Kelleners
Brian L. Kelly
Henry A. Kissinger
John E. Klein
*C. Jeffrey Knittel
Joseph Konzelmann
Franklin D. Kramer
Laura Lane
Almar Latour
Yann Le Pallec
Jan M. Lodal
Douglas Lute
Jane Holl Lute
William J. Lynn
Mark Machin
Marco Margheri
Michael Margolis
Chris Marlin
William Marron
Christian Marrone
Gerardo Mato
Erin McGrain
John M. McHugh
*Judith A. Miller
Dariusz Mioduski
Michael J. Morell
*Richard Morningstar
Georgette Mosbacher
Majida Mourad
Virginia A. Mulberger
Mary Claire Murphy
Edward J. Newberry
Franco Nuschese
Joseph S. Nye
Ahmet M. Ören
Sally A. Painter
Ana I. Palacio
*Kostas Pantazopoulos
Alan Pellegrini
David H. Petraeus
*Lisa Pollina
Daniel B. Poneman
*Dina H. Powell McCormick
Michael Punke
Ashraf Qazi
Thomas J. Ridge
Gary Rieschel
Lawrence Di Rita
Michael J. Rogers
Charles O. Rossotti
Harry Sachinis
C. Michael Scaparrotti
Ivan A. Schlager
Rajiv Shah
Gregg Sherrill
Jeff Shockey
Ali Jehangir Siddiqui
Kris Singh
Walter Slocombe
Christopher Smith
Clifford M. Sobel
James G. Stavridis
Michael S. Steele
Richard J.A. Steele
Mary Streett
*Gil Tenzer
*Frances M. Townsend
Clyde C. Tuggle
Melanne Verveer
Charles F. Wald
Michael F. Walsh
Ronald Weiser
*Al Williams
Maciej Witucki
Neal S. Wolin
*Jenny Wood
Guang Yang
Mary C. Yates
Dov S. Zakheim

HONORARY DIRECTORS
James A. Baker, III
Robert M. Gates
James N. Mattis
Michael G. Mullen
Leon E. Panetta
William J. Perry
Condoleezza Rice
Horst Teltschik
William H. Webster

**Executive Committee Members*

List as of November 18, 2022



1030 15th Street, NW, 12th Floor,
Washington, DC 20005
(202) 778-4952
www.AtlanticCouncil.org