MAY 2023

Evolving Cyber Operations and Capabilities

EDITORS
James A. Lewis
Georgia Wood

AUTHORS
James A. Lewis
Erica D. Lonergan
Julia Voo
Melanie Garson
Amy Ertan

A Report of the CSIS Strategic Technologies Program

CSIS | CENTER FOR STRATEGIC & INTERNATIONAL STUDIES

MAY 2023

Evolving Cyber Operations and Capabilities

EDITORS

James A. Lewis

Georgia Wood

AUTHORS

James A. Lewis

Erica D. Lonergan

Julia Voo

Melanie Garson

Amy Ertan

A Report of the CSIS Strategic Technologies Program

CSIS | CENTER FOR STRATEGIC & INTERNATIONAL STUDIES

About CSIS

The Center for Strategic and International Studies (CSIS) is a bipartisan, nonprofit policy research organization dedicated to advancing practical ideas to address the world's greatest challenges.

Thomas J. Pritzker was named chairman of the CSIS Board of Trustees in 2015, succeeding former U.S. senator Sam Nunn (D-GA). Founded in 1962, CSIS is led by John J. Hamre, who has served as president and chief executive officer since 2000.

CSIS's purpose is to define the future of national security. We are guided by a distinct set of values—nonpartisanship, independent thought, innovative thinking, cross-disciplinary scholarship, integrity and professionalism, and talent development. CSIS's values work in concert toward the goal of making real-world impact.

CSIS scholars bring their policy expertise, judgment, and robust networks to their research, analysis, and recommendations. We organize conferences, publish, lecture, and make media appearances that aim to increase the knowledge, awareness, and salience of policy issues with relevant stakeholders and the interested public.

CSIS has impact when our research helps to inform the decisionmaking of key policymakers and the thinking of key influencers. We work toward a vision of a safer and more prosperous world.

CSIS does not take specific policy positions; accordingly, all views expressed herein should be understood to be solely those of the author(s).

Acknowledgments

This report is made possible by generous support from the UK National Cyber Security Centre.

Center for Strategic & International Studies
1616 Rhode Island Avenue, NW
Washington, DC 20036
202-887-0200 | www.csis.org

Contents

Introduction

BY: JAMES A. LEWIS

Most networks can be breached, and most software has exploitable flaws. This can give unparalleled advantage to attackers, but the situation in Ukraine suggests that an energetic and thorough defense can prove more than adequate in matching this advantage. The Ukraine experience can guide decisions on cyber defense, and it suggests that adequate cyber defense will require different approaches, involve new actors, and be complex for nations to construct and coordinate. As part of the UK National Cyber Security Centre's efforts to shape debate and discussion around cybersecurity issues, this collection of essays examines the war in Ukraine, with a view to the wider debate around the role and value of cyber capabilities.

The "information space" is one of the key spaces in this conflict. Both sides have vied to shape public narratives and international opinion. Much has been written about the West's use of the rapid declassification of strategic intelligence to counter and debunk Russian lies about actions in Ukraine. Similarly, much debate amongst academics and commentators has sought to understand whether or not the world is witnessing "cyber war" in Ukraine, or whether and how cyber operations add value to furthering a state's strategic objectives. Originally, this discussion had a focus on cyber's offensive utility. The following essays shift the focus toward the use of cyber capabilities for defensive or protective purposes and look at the Ukraine conflict through the lens of cyber defense to identify critical lessons from Ukraine on the construction of cyber resilience.

Serious thinking about cyber defense has largely transitioned from giving deterrence a central place in defensive strategies to focusing on the concept of resilience. Democracies cannot expect to deter adversaries from attempting to use cyber operations to advance their national objectives. This leads to the conclusion,

discussed in all of the essays, that the goal for national policy must be cyber resilience: the ability to minimize disruption to critical data and services. Advocating for deterrence still serves a political purpose by signaling a desire to avoid conflict, but it is no longer the foundation of national cyber defense.

A good example of this is the new national cyber strategy published in March by the United States. The strategy never uses the word "deterrence" because, in the view of those responsible for its drafting, deterrence had failed routinely in cyberspace. Deterrence assumes that an adversary can be dissuaded from action; resilience assumes that adversary cyber action is inevitable. This has led to the conclusion that resilience is a better approach to cyber defense, particularly against a range of adversaries we confront, which includes not only states but also criminals and proxy forces. In this sense, cyber resilience protects against a much wider–and future–set of threats.

These essays explore different aspects of defense and resilience–including the actors that contribute to it–and identify lessons that Western countries can draw from the Ukrainian experience to build robust, collective cyber resilience. This includes the power of partnerships, whether in responding to cyberattacks or ensuring the continuation of vital services amidst conflict, and the unprecedented coalition of government, multinational, industry, and civil society actors whose efforts have enabled a stronger Ukrainian defense.

It should be noted that the most important aspect of resilience is only discussed indirectly in the essays: the need for political and social resilience. Lonergan, for example, notes that the political implications of cyber actions have proven to be more important than their military effect. One of Putin's many miscalculations was the belief that Ukrainian defenses would quickly crumble. A Russian analyst (now in exile) suggests the precedent of Afghanistan as shaping Russian expectations, since in that case a well-equipped and Western-trained army evaporated in a matter of a few weeks. Putin may have expected Kyiv to react like Kabul. However, Ukraine's leaders and people were not ready to concede to Russian suzerainty. The keystone of resilience is the political will to continue to resist. While it can be an elusive term, this political will forms the basis for diplomacy and defense.

The essays point out that the Ukraine conflict demonstrates that political resilience must be strengthened in cyberspace, by attention to both the digital technologies that create the information space messages and the content itself. This is not only because of the struggles over the narratives that shape opinion (and thus political will), nor solely because of the possibility of disrupting critical infrastructure, but also because cyber actions provide the tools and the structure to build a resilient community for defense–a community, as the authors note, that has transcended the boundaries of Ukraine and Russia.

There is more to cyber resilience than political will, of course (although without political will other actions are superfluous)–people, technology, organization, planning. Nor can cyber resilience be thought of as solely the remit of government. Indeed, what the Ukraine conflict has demonstrated is the broad, diverse range of actors participating in a conflict.

A more diverse set of participants in the conflict raises questions of how it is that the roles and responsibilities within cyberspace are understood, as well as what the norms and rules are that dictate how actors conduct themselves. Ukraine has demonstrated the value of coalitions in cyberspace, and of collective defense, including robust and distributed data and network architectures. Partnerships with civil society, the private sector, and other governments are crucial. Organizing this multi-party effort requires an ability to connect and communicate with all actors, and this requires reinforcing established channels for media and official

communications with the use of distributed and decentralized messaging services, like Signal and Telegram. All of the essays explore the new digital landscape where cyber conflict will occur and which nations must defend: a landscape created by fiber optic networks, mobile telephony, the "cloud," and satellites.

The essays draw several lessons from the Ukrainian experience. The first is that many cyber strategies, in light of that experience, can now be seen to be incomplete or inadequate in their definitions of what is critical for defense. A second is the need to establish deep relations with allied and partner nations for sharing intelligence, technology, and tactics. Ukraine had an advantage in that its cyber conflict with Russia began in 2014, allowing government agencies to develop greater collaboration in responses and Ukraine to build mature relationships with allies. Similarly, establishing relations with global service providers and civil society on an ongoing basis is critical. The ability to use resources and support from the private sector and civil society gave Ukraine an advantage in defense that Russia was unable to match.

The authors recognize the need to exercise a degree of caution in drawing on the Ukrainian experience. Russia's military proved to be startlingly incompetent; future opponents may not be similarly afflicted. Russia's brutal and unprovoked invasion created a wave of sympathy and support among democracies and civil society. Other conflicts, where moral and ethical distinctions are not as stark, may not produce the same response. One task for national cyber agencies is to build now the supportive relationships with nongovernmental actors that are needed for conflict: both the constant ongoing low-level conflict that defines cyberspace and the eventuality of a conflict that crosses the threshold of the use of force, something that seems much closer than it did a decade ago.

The essays included in this collection predict that many different categories of actors will be enmeshed in future cyber conflict. This aspect of the Ukraine conflict provoked a confusing discussion in the broader cybersecurity literature on the legality of using proxies and the implications for the global norms on responsible state behavior in cyberspace that were agreed upon at the United Nations. Frankly, this debate seems to be based on misunderstanding. The UN discussions made it clear that the agreed norms do not apply during armed conflict—which is the sphere of different norms and laws, in particular the Laws of Armed Conflict (LOAC). There are ambiguities, of course, created by the nature of cyberspace when nations attempt to apply LOAC, given that distinctions among participants and targets that can be clear in the physical world are opaque in cyberspace, but the authors discuss whether the use of proxies and militias has become a normal and (if done in accordance with LOAC) legal part of warfare and most likely an element of any cyber conflict in the future.

The essays raise these points in greater detail and clarity. Lonergan's discussion of proxies makes the important point that while there is little evidence of effect from "hacktivism" on opponent decisionmaking or military capabilities, there is strong evidence that the primary effect is political and international—to build a community of support and to shape the narrative of the conflict for national and international audiences. The proxy actors' apparent relationship with the "sponsoring" state is a key determinant of this, combined with a greater international orientation to shape the narratives of the conflict, and a focus solely on cyber effects may miss the most important impact created by proxies. Lonergan criticizes the tendency among policymakers and media to default to hyperbolic language to depict the effect of proxies, regardless of their true impact—noting that hyperbolic rhetoric about cyber proxies only reinforces their narratives and becomes a tool to rally their constituencies.

Voo's essay notes that the internet has become a political battleground and that Ukraine offers important strategic lessons for the key foundations of successful cyber defense. She asks fundamental questions of whether the responsibility for defense lies in the voluntary actions of tech companies or whether special rules

for social media, dual-use technology, and the participation of volunteers are needed in periods of conflict. She emphasizes the need for organization and the importance of integrating cyber defense strategies into a country's wider military and intelligence strategies.

She and Ertan both note that private sector actions are not driven solely by altruism, since Russia's cyber actions harm the space in which they do business, and there is only an ad hoc business model for private sector actions. Voo asks what has become the central question for international cybersecurity: whether consequences are needed for norms to have any meaning. Ertan suggests that countries may need to develop (individual or collective) funding mechanisms to remedy this with suggestions for remodeling cyber resilience from a NATO allies perspective. She also makes the critical point that "cyber war" is a flawed concept, since most adversary action remains below the use-of-force threshold. The increasing ease with which authoritarian states use cyberspace to undermine a rules-based order creates an uneasy space that is marked by conflict rather than peace. Garson also points to early misunderstandings of the complexity and limitations of cyber operations that confused expectations for the Ukraine war. She explores the sheer depth of the private sector's involvement in cyberspace, along with the complexity this creates for companies as they seek to navigate engagement and risks within complex geopolitical crises—as well as the implications that the private sectors' actions hold for long-term stability in cyberspace, as the lines between defensive and offensive activity become increasingly blurred in conflict.

These brief synopses do not do justice to the essays, and indeed barely touch upon many of their most salient points. There are also the caveats that the conflict has not ended and that the full details have not emerged. But with these caveats, the essays provide a deeper understanding of the use of cyber operations in the war—and how democratic countries should, in light of this, prepare their cyber defenses and resilience, whether within or outside of a conflict.

The Implications of Cyber Proxies in the Ukraine Conflict

BY: ERICA D. LONERGAN

Introduction

In the lead-up to Russia's invasion in February 2022, much of the expert commentary within the cyber community about the Ukraine conflict focused on three things: the extent to which Russia would launch a cyber "shock and awe" campaign to coerce Ukraine into submission; fears of a Russian cyber onslaught against the United States, the United Kingdom, and Europe to deter Western intervention or retaliate against economic sanctions; and speculation about the degree to which Russia would effectively integrate cyber and kinetic operations on the modern battlefield.[1] Yet, after more than one year of war, none of these issues has been a defining feature of the cyber dimension of the conflict in the way that most analysts expected.[2] Instead, one of the most significant cyber features of the war has been the role of third-party actors as belligerents—cyber proxies—aligned to Russia or Ukraine. While the concept of cyber proxies is not novel, it has taken new and evolving characteristics in the context of the Ukraine conflict, offering a potential preview of how cyber proxies may play a role in future crises and conflicts.

Moreover, an important feature of cyber proxies in the Ukraine conflict is their willingness to conduct cyberattacks beyond the theater of operations, including against the United States, the United Kingdom, and Europe. While policymakers issued warnings about potential Russian cyberattacks that might spill over beyond Ukraine, they did not necessarily anticipate the form in which they would ultimately occur—specifically, low-impact, disruptive cyber activity carried out by hacktivist groups. For instance, in late January 2022, the National Cyber Security Center (NCSC) in the United Kingdom cautioned that Russia was likely to target the private sector via cyber means and advised companies to "bolster their cyber security resilience in response to the malicious cyber incidents in and around Ukraine."[3] And in February 2022, the U.S. Cybersecurity and

Infrastructure Security Agency (CISA) issued a stark warning to private companies that Russia has "used cyber as a key component of [its] force projection over the last decade . . . The Russians understand that disabling or destroying critical infrastructure—including power and communications—can augment pressure on a country's government, military, and population and accelerate their acceding to Russian objectives."[4] However, Russian advanced persistent threat actors have largely avoided conducting major, significant cyberattacks against Western targets.[5] Instead, there has been a significant volume of disruptive cyber activity carried out by proxy actors with far more ambiguous relationships to the Russian government.

The prevalence of cyber proxy groups was immediately apparent in the opening days of the Ukraine conflict. For example, on February 24, 2022, the Anonymous hacker collective declared via its Twitter account that it was "currently involved in operations against the Russian Federation. Our operations are targeting the Russian government."[6] Shortly after that, Killnet, which was previously a modest hack-for-hire group, morphed into a politically motivated hacktivist entity and began a sustained effort to conduct low-cost, disruptive cyberattacks against a range of Western targets.[7] Around the same time, the newly established IT Army of Ukraine, a volunteer hacker army that includes individuals from Ukraine and around the world, began to launch attacks against targets within the Russian Federation.[8] In other words, the Ukraine conflict is characterized by a notable resurgence of proxy warfare—but with novel characteristics and permutations. Specifically, many of these cyber proxy groups are operating more as transnational social and political actors—creating platforms for political mobilization and influence—than as traditional proxies conducting cyber effects operations on behalf of a state government for the purposes of coercion or warfighting.[9]

In light of the reality that cyber proxies are a consistent feature—not an aberration—of this conflict, governments should anticipate that future wars may give rise to similar patterns. Yet, policymakers seem to be overlooking this aspect of the war, instead focusing more on dissecting the causes of Russia's apparent underperformance in cyberspace or on emphasizing their own roles in contributing to Ukraine's cyber defenses.[10] However, because a significant portion of the cyber activity occurring in the context of this war is being perpetrated by different types of cyber proxy actors, it is important for policymakers to assess the implications of the novel ways in which cyber proxies are influencing the Ukraine conflict to better anticipate their roles in future contingencies.

Traditional Concepts of Cyber Proxy Warfare

The notion of "proxy war" in cyberspace is not a new phenomenon. Indeed, governments have formed ambiguous, plausibly deniable relationships with a variety of cyber actors—both witting and unwitting—for as many decades as cyber conflict has existed. These actors range from criminal organizations at varying levels of sophistication (such as a ransomware groups); to patriotic hackers or hacktivists; to private firms; and to advanced persistent threat actors with closer, but still plausibly deniable, relationships with governments.[11] Most discussions of cyber proxies focus on the different ways in which states direct (with varying degrees of overtness) or enable non-state actors to conduct cyber operations on behalf of or aligned with the interests of the state.

Russia has been an especially prolific actor in the cyber proxy realm, leveraging these groups not only for cyber effects operations but also for broader purposes of information and psychological warfare. This is not surprising given the Russian doctrine, which conceptualizes cyberspace and cyber warfare as only one element of a broader "information confrontation."[12] For example, Moscow has established longstanding relationships with cyber criminal organizations: providing them safe haven, protecting them from prosecution, and turning a blind eye to their criminal activities in exchange for their tacit agreement

to avoid targeting Russian interests in cyberspace and to be available when called upon to act on behalf of the government.[13] More recently, Russia has permitted ransomware groups to operate from its territory and conduct costly attacks against Western targets (even if it does not direct or order them to do so), including the spate of ransomware attacks in 2021 against U.S. firms such as Colonial Pipeline and JBS meat processing.[14] Yet, Russia's tolerance of cyber criminal groups is sometimes tested, such as its announcement in January 2022 that the Federal Security Service (FSB) had dismantled the ransomware group REvil, arresting some of its members and seizing its assets.[15]

Russia has also leveraged both witting and unwitting cyber proxies to complement its military campaigns. As part of Russia's 2008 invasion of Georgia, it is likely that the Russian government facilitated the creation of online forums to distribute malware and coordinate cyberattacks against Georgian targets.[16] Cyber proxy groups were also prolific in the context of Russia's 2014 annexation and occupation of Crimea.[17] For example, in October 2014 the hacktivist group CyberBerkut, which experts suspect has connections to APT28 (the Russian advanced persistent threat actor linked to the GRU, Russian military intelligence), compromised Ukraine's election systems and posted exfiltrated data online just prior to the parliamentary elections.[18] And in 2015, APT28 carried out the first-known cyberattack against a state's power grid, disrupting Ukraine's grid for several hours during the winter.[19] It is likewise notable that Ukrainian patriotic hacker groups were also active during Russia's 2014 military campaign—such as the Ukrainian Cyber Army, which conducted website defacements and similar types of low-impact attacks.[20]

Historically, states have found working with cyber proxy groups appealing for a range of reasons. The ambiguous and secretive nature of these relationships enables governments to plausibly deny their role in cyber incidents, shielding themselves from potential retaliation by adversaries or from paying political costs in the context of their own domestic politics. In some cases, a government may see benefits in tacitly permitting proxy groups to engage in more aggressive, disruptive, or offensive actions than it would otherwise be willing to conduct directly, or it may permit them to attack certain types of targets that the government might otherwise see as being off limits for its own cyber forces, such as civilian critical infrastructure. Encouraging action by cyber proxy groups can also serve as a means of diverting domestic political or nationalist pressure during international crises, acting as a form of pressure release.[21] Permitting cyber proxies can also keep potential threats to a regime busy: rather than applying their cyber skills against the government, would-be hackers can be directed against both internal rivals and external threats to a regime. Additionally, particularly for less mature cyber powers, proxy groups can provide a much-needed augmentation of a state's cyber capabilities or skilled personnel. In some cases, highly organized cyber criminal enterprises may be more sophisticated than some nation-state actors. From the perspective of the cyber proxy group, implicit or explicit state support provides a number of benefits. Most importantly, the legal protections offered by states can shield proxy groups from prosecution or even extradition by international law enforcement, enabling groups to carry out their enterprises without scrutiny. Cyber proxies may also perceive gains from resources, technologies, training, and capabilities to which they might otherwise lack access.

Yet, there are also risks. In particular, with respect to the state, cyber proxy groups could exceed their mandate, creating risks of blowback or retaliation against the government or increasing the chances of inadvertent escalation. In a different vein, cyber proxies may simply be ineffective, shirk responsibilities, or divert government resources toward their own desired objectives. Finally, cyber proxies could turn against their state sponsor, engaging in cyber activities that directly or indirectly undermine the sponsor's interests or political stability. Therefore, a core aspect of cyber proxy warfare hinges on the nature of the relationship between the proxy group and the state sponsor. The extent to which a state has effective command and control over the

activates of a proxy group—directing it to conduct cyber operations in its interests—or whether it risks both under- and over-performance by a proxy shapes the benefits and risks of working with cyber proxies.

Traditional Forms of Cyber Proxy Behavior in Ukraine

The 2022 Ukraine conflict has seen a significant amount of this type of traditional cyber proxy behavior—where a state implicitly permits or more directly urges affiliated non-state actors to conduct cyberattacks.[22] In this sense, the current conflict reflects a level of continuity with Russia's past approaches. One example of traditional cyber proxy warfare is the failed attempt by APT28 on April 8, 2022, to replicate its 2015 success in disrupting Ukraine's power grid.[23] While ultimately unsuccessful (Ukraine's Computer Emergency Response Team and a Slovakian cybersecurity firm were able to halt the attack)[24], it appears to have been an effort by Russia to apply cyber power as part of a broader warfighting approach via leveraging traditional proxy groups. Indeed, evidence indicates that the attackers had gained access to the power grid's system in the first phases of the conflict.[25]

The Ukraine conflict has also been characterized by the activation of Russian-aligned hacktivist groups with more ambiguous relationships with Moscow that are likely under much looser command and control structures—similar to Russia's mobilization of these groups in 2008 in Georgia and 2014 in Crimea. Indeed, many of these groups claim to have no formal affiliation with the Russian government, even as they operate in Russia's interests. Specifically, these Russian-aligned hacktivist groups have been active in attacking targets of interest within Ukraine, including critical infrastructure, even if the sophistication and severity of their attacks has been minimal. For example, on August 15, 2022, the People's CyberArmy conducted a distributed denial of service (DDoS) attack against a Ukrainian state-owned nuclear power company, Energoatom. The hacktivist group unleashed 7.25 million bot accounts, which flooded the power company's website with bogus traffic. Nevertheless, Energoatom was able to thwart the DDoS attack within a few hours, and the People's CyberArmy quickly moved on to other Ukrainian targets.[26] In another illustrative example, on July 1, 2022, XakNet, a Russian-aligned hacktivist group, claimed that it had conducted a cyberattack against DTEK, Ukraine's largest energy holding company, posting to its Telegram channel screenshots that were meant to serve as proof of its successful breach of the company's networks.[27] This cyber incident occurred at the same time as Russian missile attacks against DTEK's Kryvorizka thermal power plant in Kryvyi Rih, although the connection between the cyber and kinetic incidents is likely spurious.[28]

New Forms of Cyber Proxy Warfare

At the same time, the Ukraine conflict is revealing new permutations of cyber proxy warfare that are more internationalized, just as the broader conventional conflict itself has drawn in multiple external participants. Specifically, a significant portion of the cyber activity that is taking place in the political context of the Ukraine conflict is being carried out by hacktivist groups that are attacking targets beyond the theater of operations—either within the Russian homeland or against targets in the West, especially the North Atlantic Treaty Organization's (NATO) member states. Moreover, these groups are drawing on participants from around the world who are aligned to their political orientation, even if they may lack the level of skill and sophistication of other threat actors, such as APT28, that are more directly aligned with governments. Examining just two different examples of these types of cyber proxy actors—Killnet and the Ukraine IT Army—reveals some of the similarities as well as the variation across these groups and how they are changing the nature of cyber proxy warfare.

In particular, while these two groups express diametrically opposed political orientations and differ in the extent of their affiliation with a government (the Ukraine IT Army was initially created by a government official, while Killnet claims to be independent of Moscow), they are primarily focused on conducting disruptive or nuisance cyber campaigns against targets beyond the battlefield in Ukraine. Additionally, both cyber proxy groups maintain active social media forums where they provide direction to their members about planning and executing cyberattacks. But these forums also serve to communicate political messages and act as a form of virtual political mobilization, rallying cadre around a cause and shaping the narrative of the conflict.

It is this combination of more internationally-oriented membership and targeting, coupled with the use of cyberattacks as a vehicle for political mobilization, that makes this form of cyber proxy warfare particularly interesting and novel in a warfighting context. In this sense, these cyber proxies act as both transnational and local actors—conducting operations beyond the battlefield as a means of cultivating their own internal political narratives, while at the same time shaping broader narratives about the conflict. In other words, these groups are playing a role in the Ukraine war not simply by virtue of how their cyber effects operations are impacting the course of the conflict, or through deterring or coercing external parties. After all, the types of operations these groups conduct are low-cost, disruptive cyberattacks that do not do much in the way of damage. Rather, their cyber campaigns are a way for groups to further political narratives about the war and shape the perceptions of different audiences, and it is through this lens—not that of cyber effects—that their impact can be best understood

Killnet

Killnet, a Russian-aligned hacktivist group that became active in the initial stages of the conflict, is a formerly small and obscure botnet for hire organization that has since rebranded as an internationally known hacktivist group. Politico has described the group as "more like an angry, nationalist online mob armed with low-grade cyber-offensive tools and tactics," contrasting it with more sophisticated Russian threat actors.[29] Indeed, Killnet's adherents are not particularly skilled and the group almost exclusively conducts straightforward DDoS campaigns, publishing simple scripts on its social media channels for followers to use.[30] Yet, Killnet has received a significant amount of attention from analysts and the media due to its near-routine targeting of Western entities, including critical infrastructure. This distinguishes Killnet from other pro-Russia hacktivist groups, which have largely focused on targets within Ukraine, perhaps in coordination or at least alignment with Russian conventional military operations.[31]

For example, in early February 2023, Killnet launched a wave of DDoS attacks against more than a dozen hospitals in the United States. But, like many of Killnet's prior disruptive attacks, the actual impact on U.S. hospitals was minimal. According to Cloudfare, the largest of these attacks peaked for only ten seconds, with the total attack lasting for only six minutes.[32] Similarly, the American Hospital Association stated that the "impact appears to have been minimal and temporary."[33] This cyber activity is a hallmark of Killnet's approach: conducting low-impact disruptive cyber campaigns against Western critical infrastructure and other targets. In these types of campaigns, Killnet does not appear to be focused on actually having an impact with its disruptive attacks—or at least does not particularly care if its self-generated bravado matches reality. Despite the negligible effects of its cyber operations, Killnet appears to relish in hyperbolic and triumphalist language to rally supporters around its cyber campaigns.

Against smaller countries, particularly the Baltic states, Killnet has been more successful in sustaining disruptive attacks over longer periods of time. For example, in May 2022 as part of its declaration of "war" against countries

supporting Ukraine, Killnet launched DDoS attacks against dozens of targets in Latvia, a NATO member state, ranging from government and transportation to finance. Accompanying these attacks were calls on Killnet's Telegram channel and other social media sites for cadre to carry out additional cyberattacks against Latvia. Killnet targeted Latvia again in July with a large disruptive attack—including a 12-hour disruption of Latvia's public broadcasting center—after the government stated it would take down Soviet-era monuments. August saw another disruptive attack, this time against the website of Latvia's parliament after the body declared Russia to be a state sponsor of terrorism. All this followed a 10-day wave of DDoS attacks against Lithuania in June in response to that government's decision to block certain Russian exports.[34] Moreover, these represent only a handful examples of the disruptive attacks conducted by Killnet and similar groups against Latvia and Lithuania which, along with Estonia, are routinely targeted in this manner by cyber proxies.

In some ways, the bluster may be the point. Specifically, an important aspect of Killnet's success as an organization derives from its Telegram channel and associated media sites, where members routinely congratulate one another and even leverage Western media reports about their cyberattacks to bolster their credibility internally and improve morale within the group.[35] Killnet's Telegram channel, which is only in Russian, has over 90 thousand subscribers.[36] Indeed, as Dark Reading reported, Killnet has seen a significant increase in its social media followers stemming from the public nature of its DDoS campaigns (even as they are not causing any meaningful effects): "Killnet's' pro-Russian DDoS crusade has also begun attracting many more followers and fans."[37] Killnet has even become a feature of Russian war-related pop culture. Last summer, Russian rapper Kazhe Oboyma published a song glorifying Killnet called "KillnetFlow (Anonymous diss)." In October 2022, Killnet launched a jewelry collaboration with Russian jeweler HooliganZ, and the group also sells other Killnet-branded merchandise. This "serves as a form of propaganda, helping to recruit new members and promote the group's cause."[38]

Like other Russian-aligned hacktivist groups, Killnet's leader, Killmilk, staunchly disavows any formal relationship with the Russian government and claims that the group is entirely self-organized and sustaining.[39] Yet, it is clear that Killnet is serving Russia's broader political purposes in the conflict. The fact that Killnet's Telegram channel is only published in Russian, for instance (coupled with its attempts to gain a foothold in broader Russian culture), provides insights into the audience the group is interested in mobilizing—domestic Russian or near-abroad Russian speaking audiences. In this sense, Killnet is ostensibly a useful tool of Moscow's efforts to maintain domestic support around continuing Russian military involvement in Ukraine—while at the same time keeping potential spoilers and discontented would-be cyber actors busy. This aligns with recent research on the use of cyber proxies during international crises, where states have been found to use these actors as a means of placating certain domestic political audiences.[40] While that research was focused on the role these groups play in facilitating the de-escalation of crises, it reflects an important insight that there are domestic political considerations in the use of cyber proxy groups that may be as significant to a government, if not more so, than international ones.

The IT Army of Ukraine

While Killnet and the IT Army of Ukraine are on opposite political sides of the conflict and engage vastly different audiences, there are several important similarities between the two groups. This is suggestive of emerging trends in cyber proxy warfare stemming from the Ukraine conflict. Both the IT Army of Ukraine and Killnet have transnational characteristics in terms of the international representation of their volunteers and the scope of their targeting. Specifically, both groups focus their efforts on attacking targets—such as civilian critical infrastructure—outside of the theater of operations in Ukraine. While Killnet largely conducts DDoS

attacks against the West, the IT Army of Ukraine has directed its efforts almost exclusively against Russian targets within the Russian Federation (rather than on the battlefield), as well against Belarus. Additionally, both Killnet and the IT Army prefer low-cost, disruptive cyberattacks, likely because this enables wider participation by would-be volunteers, making it easier for sympathetic individuals to join the cause. Finally, both groups leverage social media platforms (albeit in different ways) as part of their efforts to facilitate political mobilization and shape the information narratives around the war.

Yet, there are also key differences between the groups. One important distinction is the nature of each group's relationship with government—a core element of cyber proxy warfare. While it is clear that the Russian government benefits from Killnet's activities, there is no evidence of a formal link between the two. In contrast, while the Ukrainian government has publicly denied any role in the IT Army's activities, the group was initially created in February 2022 by Ukraine's deputy prime minister and minister of digital transformation, Mykhailo Fedorov, reportedly at the suggestion of Yegor Aushev, a Ukrainian tech entrepreneur.[41] Moreover, in March 2023, the Ukrainian government announced that it is in the process of developing legislation to formalize the IT Army and incorporate it into the country's regular armed forces.[42] Additionally, there is far less plausible deniability in the relationship between Kyiv and the IT Army.[43] As Newsweek depicts it, the Ukrainian government "is the first country, certainly the first European democracy, to openly embrace a hacktivist militia during a shooting war."[44] Similarly, Wired describes the IT Army as "a government-led volunteer unit that's designed to operate in the middle of a fast-moving war zone."[45] That said, it is important to note that the idea of a decentralized volunteer cyber citizen militia is not an entirely novel concept in Europe, with the exemplar being the Estonian Defence League's Cyber Unit.[46]

In fact, while IT Army maintains that it operates independently of the Ukrainian government (at least until the new legislation is passed), researchers have suggested that the organization is actually segmented into two distinct groups. The first is a large, public-facing, globally engaged network of volunteers who conduct disruptive cyber operations against Russian targets. Notably, however, the size of its membership has been declining over time, estimated to be nearly 300,000 subscribers in February 2022 to just under 200,000 in March 2023.[47] The second element of the IT Army is an "in-house team likely consisting of Ukrainian defense and intelligence personnel that have been experimenting with and conducting ever-more complex cyber operations against specific Russian targets."[48] This latter component, therefore, embodies a traditional concept of cyber proxy warfare (characterized by plausibly deniable connections between military and intelligence organizations and cyber actors), while the former resembles newer permutations of cyber proxies.

Additionally, the IT Army of Ukraine is far more disciplined than Killnet in terms of its organization and approach, professing to be deliberate in its targeting decisionmaking. For example, in response to a query from a Newsweek reporter, an IT Army spokesperson noted that the group is "focused on causing economic damage to Russia in order to weaken its ability to wage war against Ukraine . . . We do not target ordinary citizens, and we take great care to adhere to the laws of armed conflict."[49] The group has developed mechanisms for organizing and prioritizing different types of targets, identifying the anticipated level of skill that a given attack demands, and coordinating and deconflicting among different efforts.[50] Its Telegram channel also maintains a routinized tasking process for disruptive attacks, where marching orders are given at the same time each day (0900 Central European Time) and targets are typically organized by a theme (such as food delivery services on a weekend to make everyday life slightly more difficult for Russian citizens—suggesting the IT Army may indeed sometimes target ordinary civilians). Despite this level of organization—ostensibly more so than Killnet—there is little evidence that the IT Army's disruptive cyberattacks are having any meaningful impact on the Russian government's decisionmaking or on the Russian population's support for the war.

This suggests that, like Killnet, the cyberattacks themselves (and, by extension, their effects) do not represent the primary contribution of the IT Army to the broader conflict. Instead, the IT Army of Ukraine has leveraged social media to create both a local (Ukrainian) and international (largely Western) community of supporters aligned with its cause. The act of collectively conducting relatively simple cyberattacks thus builds and reinforces community, providing something around which to rally and energize supporters. How these two groups use their social media platforms is also suggestive of the different audiences they are aiming to mobilize. Killnet's Telegram page is focused on shaping the perceptions of Russian-speaking audiences. In contrast, the IT Army's Telegram page is in both Ukrainian and English, which reflects the Western-oriented audience the group aims to engage. Indeed, while the group's first Telegram post on February 26, 2022, was in Ukrainian, the second was in English and contained the following message: "For all IT specialists from other countries, we translated tasks in English. Task # 1 We encourage you to use any vectors of cyber and DDoS attacks on these resources."[51] What followed was a list of Russian targets organized by sector, from "business corporations" like Gazprom and Lukoil, to "banks" such as Sberbank, and to "the state" including the Office of the President, the Ministry of Defense, and others. In this sense, the IT Army of Ukraine is a microcosm of Ukraine's broader effort to shape the information environment within Ukraine and—importantly—among Western audiences, whose political support is essential for enabling military support to the country.

Policy Implications

Several policy implications follow from this analysis. One clear finding is that future crises and conflict are almost certain to involve a range of cyber proxy actors that are diverse in terms of their level of skill, connection to a central government, and willingness to engage different types of targets. Some of the cyber proxies aligned to the Russian government have conducted (or attempted to conduct) more sophisticated attacks against key targets in Ukraine; others have engaged in low-cost attacks within Ukraine; and still others have conducted disruptive attacks beyond the theater against Western targets.

Some have argued that the proliferation of cyber proxy behavior in the context of the Ukraine conflict has negative implications for international norms about state sponsorship of cyber proxy groups.[52] Western states have sought to promote a norm that states should be held accountable for any cyberattacks that they enable or permit by failing to restrain or turning a blind eye toward proxy groups that emanate from their sovereign borders.[53] Moreover, in the March 2021 final report of the United Nations Open Ended Working Group, nearly all states have agreed to uphold norms of responsible behavior, including norms around preventing the misuse of information and communications technologies.[54] As a result, some have argued that Ukraine's public support for cyber proxy groups conducting attacks against Russia (such as the IT Army of Ukraine) "stands in stark violation of recently agreed-to norms on state behavior in cyberspace, as well as the foreign policy positions of NATO members and the European Union."[55] Yet a key challenge with this line of reasoning, as others have pointed out, is that armed conflict represents a fundamentally different context than peacetime or even times of international crisis—one in which "cyber norms should be expected to fall by the wayside before or along with the transition from IHRL [International Human Rights Law] to LOAC [Law of Armed Conflict]."[56] Therefore, policymakers should exercise discretion when considering the normative implications of this conflict and avoid muddying the waters between cyber behavior during wartime versus during routine competition—especially because this may inadvertently undermine important efforts to establish cyber norms where they are actually applicable.

Additionally, policymakers should not apply a one-size-fits-all approach to these different actors. Traditional policy tools—such as placing diplomatic pressure against state sponsors of cyber proxy groups (like Biden's

warning to Putin in June 2021 at the Geneva summit against permitting groups to conduct cyberattacks against U.S. critical infrastructure[57]) coupled with law enforcement action and disruptive campaigns, may be more effective in addressing traditional cyber proxy actors, especially those over whom a state has more effective command and control.[58] These approaches (likely together with credible threats of retaliation, such as repeated public affirmation that NATO's Article 5 applies to the cyber domain[59]) appear to have worked in dissuading Russia from directly ordering or enabling more advanced threat actors from conducting major cyberattacks against NATO member states. While speculative, it is plausible that Russia's decision to dismantle the ransomware group REvil in January 2022—just one month prior to the invasion—was in part meant as a signal to other groups of Russian control, perhaps to deter them from taking unwanted cyber action or to nudge them fall in line with Moscow's goals. One potential example of this is the February 25 statement by the Conti ransomware group on its Dark Web site that it was "officially announcing a full support of Russian government" and would respond to any "war activities against Russia."[60] This is notable because, previously, Conti was not a politically motivated actor and was instead decidedly focused on cyber crime for financial gain.[61] Indeed, the group's decision to become political caused an internal rift and likely motivated a significant leak of internal documents.[62]

However, it is unlikely that these traditional tools will be as effective against groups such as Killnet that have a more indirect relationship with central government and that draw on a more international base of support. These groups are likely to be less dependent on the safe haven provided by a government (especially because their lack of sophisticated infrastructure, reliance on open-source tools, and global membership make them relatively easy and low-cost to dis- and reassemble). This means that applying traditional levers to shape the behavior of these groups through putting pressure on state sponsors is a fruitless endeavor.

Furthermore, the impact new cyber proxy actors are having on the Ukraine conflict—more in terms of shaping political mobilization and cultivating or reinforcing narratives about the war, and less in terms of the actual effects of their cyber operations—complicates how policymakers are typically inclined to address these groups. In some ways, from a policy perspective, it is more straightforward to focus on thwarting, mitigating, or improving resilience against cyber effects operations than it is to counter political narratives or offer credible competing ones. Yet how these cyber proxies are shaping the conflict is more akin to political warfare than coercion. This relates to a broader challenge Western policymakers are facing in the context of the Ukraine war—namely, that while advanced liberal democracies are largely united and have remained more cohesive than expected in pushing back against Russian aggression, a significant part of the world is either Russian-sympathetic (such as China) or non-aligned (such as India).[63] Of course, cyber proxy groups like Killnet and the IT Army of Ukraine are only one element of the broader contest to shape the perceptions of different audiences. Nevertheless, in evaluating the impact of these groups (and, by extension, applying policies to address them) through the lens of "hackers for hire," policymakers are missing their real role in the conflict.

Additionally, there is a tendency among policymakers and media to default to hyperbolic language when depicting the workings of various cyber threat actor groups, regardless of their true stature.[64] But blustery rhetoric about these cyber proxy groups only plays into their narrative, which groups in turn use as a tool to further rally their constituencies. Therefore, policymakers should take care to avoid inadvertently playing into groups' political narratives and providing fodder that enables them to increase their own visibility within their audiences.

Finally, the recent announcement that the IT Army of Ukraine may be absorbed into Ukraine's armed forces suggests broader implications for cyber defense and resilience. The head of Ukraine's National Coordination

Center for Cybersecurity, Nataliya Tkachuk, shared with Newsweek that the government was motivated to formalize the IT Army so that the group would, "become the basis for building the state's cyber defense capabilities, engaging cyber volunteers in these activities, and creating a cyber reserve." The IT Army appears to support this effort, commenting that, "We fully trust the efforts of the working group to legalize a massive fight in the cyber sector and welcome the moment when it will stop being the grey zone. We . . . believe that the integration of the IT Army into the cyber reserve will help in building a more effective defense against cyber threats."[65] This transition is likely unprecedented. There are no known examples of an informal hacktivist group becoming incorporated into a state's regular armed forces. However, other states have employed volunteer models for cyber defense. Estonia, for example, has pioneered one approach to leveraging volunteer cyber defenders through its Estonian Cyber Defence League—which itself was created in response to Russia's cyberattacks against the country in 2007.[66] One key issue for Ukraine is how a force that had previously been conducting a largely offensive mission will be able to shift to one focused on defense, both in terms of skills and commitment to a different type of mission. The level of expertise required to carry out low-cost disruptive attacks against Russian-aligned targets is different from that which is necessary to defend domestic networks and systems. Another important question is which elements of the IT Army will transition into regular forces, particularly given the group's current international composition—as well as the extent to which the government will be able to control the activities of those elements of the IT Army that do not get subsumed under traditional command structures and prevent them from going rogue. Western policymakers should closely follow how this process unfolds in Ukraine, as it could offer important lessons for how governments could better integrate and leverage their own civilian cyber talent to improve cyber defense and resilience.

The views expressed are personal and do not reflect the policy or position of any U.S. government organization or entity.

Lessons from Ukraine's Cyber Defense and Implications for Future Conflict

BY: JULIA VOO

Introduction

More than a hundred countries reportedly possess the capability to launch state-sponsored cyberattacks. The Russia-Ukraine conflict presents a case study of two capable cyber powers applying their capabilities to achieve national objectives in direct opposition to one another over a sustained period. This conflict has illuminated an eight-year cyber struggle that escalated to include kinetic components last year. With conflicts between states now frequently unfolding in the ambiguous space between peace and war, many national governments should examine Ukraine's cyber defense as a learning opportunity. Reorganizing to better defend against cyber threats and maximizing capabilities in cyberspace was already a priority for numerous governments before this conflict. While two-thirds of governments worldwide have introduced strategies to defend against threats in cyberspace, more comprehensive measures are needed. The effectiveness of Ukraine's defense, combined with the high number of countries capable of launching offensive cyber operations, highlights the necessity for the proper structures and relationships to approach cyber defense holistically and effectively. This cyber conflict is notable for how Ukraine—with support from national governments, civil society, and the private sector—conducted a strong cyber defense against a top-tier cyber power.

It is likely that 2023 will see Russia escalating its cyberattacks against Ukraine, and perhaps NATO partners, to further its objectives.[67] While it is challenging to generalize the lessons from Ukraine's cyber defense so far, there are several key takeaways that other states should derive from the past year as they face cyberattacks from not only Russia.

Russia-Ukraine Conflict and the Value of Cyber Defense

Before Russia's invasion of Ukraine, the world had not witnessed a kinetic conflict between two highly capable cyber powers. Contrary to the anticipated crushing defeat many expected Russia to deliver to Ukraine due to Russia's extensive record as a capable offensive cyber actor, Ukraine has managed to successfully defend its interests while demonstrating the role of cyber capabilities in conventional conflict.[68] Ukraine had been encouraged for years to build its cyber defenses and implement a "whole-of-society" cyber defense. As a result, the lessons from this conflict are challenging to generalize given their specific context, including a pre-existing gray zone conflict and unprecedented resources from international actors and the private sector. Nonetheless, Ukraine's cyber defense thus far merits reflection by other national governments looking to strengthen their own moving forward.

EXPERIENCED CYBER DEFENDERS

Although Russia officially crossed into Ukrainian territory on February 24, 2022, Ukraine has been defending itself from Russian cyberattacks since Russia's illegal annexation of Crimea in 2014, with attacks escalating ahead of the invasion. Over the past decade, Ukraine's public, energy, media, financial, business, and nonprofit sectors repeatedly suffered from Russian attacks. In 2015, Russia shut off part of Ukraine's electricity grid, leaving 230,000 people without power for six hours. In 2017, NotPetya malware deployed by the GRU (Russian military intelligence) targeted hundreds of firms and hospitals worldwide, including Ukraine's power grid. Russia's cyber operations since the beginning of the kinetic conflict have ranged from preventing access to basic services to data theft, disinformation, wiper malware, DDoS attacks, phishing emails, and surveillance software. Despite these challenges, Ukraine has managed to marshal its capabilities, resources, and relationships to block and recover from setback after setback in cyberspace. A crucial component of cyber defense is investment in both financial resources and human capital to ensure the recruitment and retention of skilled cybersecurity professionals. The maturity of Ukraine's security operations and incident response, along with its battle-hardened cyber defenders, is difficult to overlook.

HOLISTIC NATIONAL CYBERSECURITY STRATEGY

More than two-thirds of countries now have some form of cybersecurity strategy to guide their overall cyber defense.[69] A notable step in Ukraine's consolidation of its national cyber capabilities was the adoption of its 2016 National Cybersecurity Strategy, which recognized the importance of all stakeholders in strengthening Ukraine's cyber defense, both inside and outside of government. National governments can increase their cyber resilience in several ways: by introducing laws and regulations on cybercrime and cybersecurity; by implementing technical measures to ensure that expertise is available to enhance cyber resilience; by establishing organizational measures to ensure coordination between government agencies and relevant actors; and by developing capacity through the growth of domestic cybersecurity industries, investments in R&D programs, and skills development. The Ukrainian government sought to enhance collaboration among all government agencies, local authorities, military units, law enforcement, research institutions, and civil society to improve Ukraine's overall cyber defense.

The most effective cyber defense strategies are integrated into a country's wider national strategies, including military operations and intelligence gathering. Furthermore, cyber strategies must be continuously updated and adapted to keep up with evolving threats and increase national resilience. Through the experience of Russia's invasion of Ukraine in 2022, there were key expansions to Ukraine's 2021 strategy that involved "a wider range of participants, including business entities, public associations, and individual citizens of Ukraine" in addressing Ukraine's national cybersecurity system.[70]

CENTRALIZATION OF GOVERNMENT CYBER DEFENSES

Increasingly, national governments are streamlining the various departments responsible for different aspects of cyber operations. There are clear roles within governments for structures such as intelligence agencies, the military, law enforcement, and the foreign service; but for cyber defense, these often separate components need to work in tandem. The 2016 Ukrainian cyber strategy also led to the creation of the National Cybersecurity Coordination Center (NCCC). The NCCC, which brings together aspects of Ukraine's National Security and Defense Council, supervises and analyzes the state of national cybersecurity, including preparedness for combating cyber threats and detecting and forecasting potential and actual threats. The NCCC also hosts international and interdepartmental training courses.[71] Ukraine's effective centralization and coordination of its governmental cyber defenses demonstrate that these capabilities need to work seamlessly together to ensure maximum effectiveness.

ALLIES SHARING INTEL AND TECH BEFORE AND DURING CONFLICT

One of the game-changing aspects of Ukraine's cyber defense is the international support it received and continues to receive. This support has come in the form of cyber expertise and intelligence from other governments, such as the United States and the United Kingdom, as well as governmental organizations like the European Union and the NATO.

International cyber partnerships and support for Ukraine started well before the February invasion. Since 2014, international partners, including the European Union, the United States, and the United Kingdom, have mobilized resources to enhance Ukraine's cyber defenses while also boosting their own. The United States and Ukraine hosted the first bilateral cyber dialogue in 2017, which included participants sharing approaches on organizing cybersecurity structures and cyber incident response procedures.[72] Since then, the United States has provided $40 million in cyber capacity development assistance to Ukraine.[73] In 2021, the European Union launched a cyber dialogue with Ukraine to strengthen its resilience and legislation in the area of cybersecurity. In the months leading up to the invasion, cyber experts from U.S. Cyber Command and Ukrainian Cyber Command conducted defensive cyber operations side by side to increase cyber resilience in critical networks.

Allies have continued to strengthen Ukraine's cyber defense since the beginning of the invasion. For example, the United States and the United Kingdom have provided intelligence briefings on Russian cyber operations, including cyber threat intelligence on potential and ongoing malicious attacks such as Industroyer2 malware, firewalls for defense, and DDoS protection. [74] The U.S. government has also assisted Ukraine with identifying and procuring hardware and software to support network defense. Notably, since the beginning of the conflict, the U.S. Agency for International Development (USAID) has supplied technical experts to support essential service providers and offered 6,750 emergency communication devices, including satellite phones and data terminals, to strengthen the resilience of critical infrastructure networks and the government.[75] After Russia invaded Ukraine in February 2022, the European Union deployed a cyber rapid response team to help with threat detection and mitigation and has provided €29 million (roughly $31 million) to increase Ukraine's cyber and digital resistance.[76] Germany has also earmarked some of its 2023 budget to defend Ukraine against Russian cyberattacks. [77]

While the full extent of Russia's cyber operations against Ukraine and NATO allies has not been made public due to the secrecy surrounding respective vulnerabilities, information sharing between Ukraine and its allies has been two-way.[78] Senior Ukrainian cyber defenders have also met bilaterally with national governments to learn from each other as the conflict continues.[79] Allies who have sent reinforcements in the form of personnel are in turn provided with expertise to better defend their own national networks against similar attacks. This

two-way learning is set to continue, with Ukraine becoming an active participant in NATO's Cooperative Cyber Defence Center of Excellence in March 2022, which, through knowledge sharing, will result in a strengthening of expertise for the alliance.

PRE-EXISTING PRIVATE SECTOR CYBER DEFENDERS

The Russia-Ukraine war has involved not only conventional military forces and proxies but also, most notably for Ukraine, technology companies. This is unsurprising, as most of the digital infrastructure in Ukraine is owned and operated by private companies. Moreover, it has long been recognized that a strong partnership between the government and the private sector is needed for robust cyber defenses.[80] The cumulative power of the private sector has enhanced Ukraine's defensive capabilities, including its ability to recover from attacks, improve its battlefield effectiveness, and enhance its global appeal.

The collaboration between the private sector and Ukraine demonstrates an unprecedented case of what is possible when there is an alignment of interests between a country at war and commercial technology companies with significant resources at their disposal and an interest in one side's victory. It remains unclear whether this is a one-off case or a harbinger for future conflicts, but the implications for policymakers are considerable.

As an example, Microsoft played a critical role in defending Ukraine against Russian cyberattacks, although it was not the only company to do so by far. In early 2022, Microsoft identified a novel trojan horse wiper malware named FoxBlade, which was aimed at Ukraine's government ministries and financial institutions. After updating its virus detection systems to block the malicious code, Microsoft contacted Anne Neuberger, the U.S. deputy national security adviser for cyber and emerging technologies, and established a secure line of communication with cyber officials to help bolster Ukrainian defenses.[81] Since then, Microsoft and others have continued to work with the U.S. government, NATO, and EU cyber officials to communicate any evidence of threat actor activity spreading beyond Ukraine.[82]

While Microsoft has been a significant contributor to Ukraine's and the wider community's cyber defense, it is only one of many private sector companies that came to Ukraine's aid. An important part of the private sector's contribution to Ukraine is not only the considerable resources received from specific entities but also the collaboration between them to jointly provide Ukraine's cyber defense. A collective of private sector and civil society organizations has volunteered to deliver and maintain Ukraine's immediate cyber defense needs since the beginning of Russia's invasion, forming a "Cyber Defense Assistance Collaborative for Ukraine" (CDACU).[83] This informal group of volunteers leveraged relationships with Ukraine's NCCC, building on pre-existing trust and rapport, to understand how the private sector could help. The CDACU received requests for assistance ranging from intelligence analysis, advice, and sharing to licenses, tactical services, and coordinated support.

BACKING UP CRITICAL DATA OUTSIDE THE ZONE OF CONFLICT

At the beginning of the conflict, Ukrainian government data was concentrated in data servers located within Ukraine as an effect of data-localization policies. However, pragmatism on Ukraine's part—acknowledging the likelihood of an attack on these servers—combined with assistance from the private sector resulted in Amazon Web Services (AWS), Google Cloud, and Microsoft migrating the data from Ukraine to servers located outside of the conflict zone to enhance resilience.[84] To defend against attacks that seek to immobilize businesses or data, it is critical to build redundancy not only in networks but also by backing up data outside of the zone of conflict. This protects data servers and facilitates rebuilding the economy at a later date. Currently, there are moves in some countries towards data localization. The example of Ukraine underlines the need to protect the physical components of cyberspace—and, in the likelihood of damage, to move data servers out of harm's way.

HACKTIVISM AND VOLUNTEERS

On February 26, Ukraine's deputy prime minister and minister of digital transformation, Mykhailo Fedorov officially announced the formation of a volunteer IT Army of Ukraine. [85] There appears to be some coordination from the Ukrainian government, and state officials have clearly encouraged their activities.[86] The creation of this 150,000-200,000-strong volunteer-organized cyber force is unprecedented.[87] The IT Army has affected more than 600 online resources in Russia, including the federal post office and pension fund, online banking, and video conference platforms. Anonymous, a hacking collective, has also declared "cyber war" on Russia and claimed credit for DDoS attacks that took down the official websites of the Kremlin and the Ministry of Defense, as well as hacking Russian state TV channels and posting pro-Ukraine content. [88] While unorthodox, Ukrainian cyber defenses have been bolstered by this volunteer force.

Looking Forward: Challenges

THE OPEN INTERNET AND INFLUENCE CAMPAIGNS

This ongoing conflict provides valuable insights into the nature of warfare across the "splinternet," where two or more internets are fragmented and governed in differing ways. In this case, Russia has a tightly controlled information space, and Ukraine is part of a more open data space. In Russia's internet space, the narrative is pro-Russia. China and a few others have aligned their narrative with Russia's. However, Ukraine's information space—part of the broader more open internet—has been the target of a stream of influence operations. [89]

The Russia-Ukraine conflict has been dubbed "the first TikTok war," highlighting the role of social media in modern conflicts. [90] Social media has not only been used by warzone citizen journalists but also by people with power and authority. Ukrainian president Zelensky, a former comedian and actor, has effectively used social media to champion the cause of Ukraine and rally international support. Russian state media has also leveraged the same platforms to disseminate fake news and propaganda. Meta, Twitter, Microsoft, Alphabet, and TikTok have all taken steps to remove their content from their platforms.[91] The Biden administration has even taken to briefing TikTok influencers on U.S. strategic goals.[92] While social media companies are instrumental in stemming the flow of propaganda, graphic material, and hate speech, questions remain. Should social media companies be solely responsible for making these decisions during a conflict? Should there be special rules during periods of armed conflict? What bodies could or should be involved in a shared oversight framework for prominent platforms? While policymakers have been grappling with these and similar questions since before the Russia-Ukraine war, the conflagration has made such issues more pressing than ever.

An open internet presents a significant challenge for national governments who support it—not only because they are more vulnerable to malign attempts to influence public opinion, but because it is not possible, nor desired, to control all information flows. Beyond considering the roles and responsibilities of platforms in the face of malign influence campaigns, there is also the question of the psychological defense and resiliency of the individual to these influences. If the convergence between information operations and cyber operations in this conflict is a new norm in cyber warfare, then building societal psychological defense, or the collective ability of society to resist foreign malign influence activities and disinformation, will likely become an institutionalized and extended part of many national cyber defense efforts in societies that intend to maintain a "free and open" internet. [93]

FUNDING PRIVATE SECTOR ALLIES

In the case of Ukraine, the private sector was willing and able to support its national defense, rapidly

influencing the situation on the ground. While the private sector's efforts have been crucial to Ukraine's defense, they have also come at a significant cost. Microsoft has spent over $400 million on the conflict and will continue to provide gratis services throughout 2023 to the tune of an additional $100 million.[94] Starlink is providing critical connectivity infrastructure to Ukraine, reportedly costing $20 million a month to maintain.[95] Amazon is backing up the Ukrainian government, critical infrastructure, and university data outside of Ukrainian territory at considerable cost.[96] Many U.S. tech companies have suspended the delivery of products and services to Russia.

The behaviors of these tech companies should not be confused with altruism. For example, Microsoft's business outside of Ukraine could be affected by spillover from the conflict, so it is in its interest to step up and defend against cyberattacks. More broadly, these predominantly U.S. tech companies could face regulatory and social backlash in key markets in the United States and Europe if they were to remain neutral or continue conducting business with Russia. Therefore, certain questions regarding the sustainability of this support remain. For one, how long will firms be willing or able to provide these critical capabilities? While U.S. secretary of defense Lloyd Austin III and UK prime minister Rishi Sunak have committed to support Ukraine for the "long haul," it is unclear whether this will also extend to supporting the private sector.[97] Further, will private sector companies request government subsidies for their efforts?[98] How will these companies decide which future conflicts to support, in kind or otherwise? And how would their bottom lines be affected by taking a more active NATO-aligned worldview? It is still not clear how long these types of firms will be willing and able to effectively donate these expensive services to Ukraine for the remainder of the conflict, or if this kind of support would be replicable for any other besieged country in the future.

CONTROLLING DUAL-USE TECHNOLOGIES

DJI, a consumer commercial drone manufacturer, has inadvertently become an arms dealer in this conflict. Both Russia and Ukraine have utilized commercially available drones, such as the DJI Mavic 3, which costs under $2,000.[99] These affordable drones have extended the range of the Ukrainian army and provided enhanced intelligence and communication capabilities. The Ukrainian army has even transformed some of these hobbyist drones into unmanned kamikaze bombers capable of carrying munitions up to 800 grams and of steering toward Russian targets.[100] While DJI announced it would halt drone sales to both Moscow and Kyiv in response to their use in the conflict, commercial drones can still be sourced from other suppliers.[101] This example of a technology that is commercial first but could be used for defense purposes presents the problem of some dual-use technologies. It also raises the issue of the difficulty for some allies to access equivalent primarily defense technologies and raises questions around how these two issues could be addressed.

FUTURE INDUSTRY ADVERSARIES

Most of the large consumer tech companies involved in this conflict are American, with the notable exceptions of Chinese-owned TikTok and DJI. However, it is worth considering an alternative scenario involving a conflict with China; how would we expect commercial Chinese actors to behave in relation to the CCP? What frameworks exist around governing tech companies in case kinetic conflict between technological superpowers (e.g., the United States and China) were to emerge? How could companies that would potentially ally with an adversary behave in such a conflict? How would cyber defenses need to adapt if equivalent consequential technology companies instead supported the adversary? What would happen if a future conflict occurred in an environment where a sympathetic private sector actor did not control various aspects of critical infrastructure?

Over 30 countries, representing more than half of the world's economy, have announced sanctions and export controls targeting Russia due to its military operations in Ukraine. These actions have impacted the

development of Russian technology and e-commerce. While sanctions against Russian technology make sense as an attempt to force compliance with international will, it is important to consider the long-term effects of exacerbating the bifurcation in technology stacks, which is largely driven by U.S.-China tensions. While bifurcation will decrease dependency, it is essential to consider the potential consequences of creating a more fragmented global technology landscape in terms of access to resources and allegiances of companies with strong links to adversaries.

ACCOUNTABILITY IS NEEDED

Negotiations at the United Nations created norms on responsible state behavior for the acceptable use of cyber capabilities. UN member states have committed to abide by 11 cyber norms.[102] These norms include interstate cooperation on cybersecurity, preventing the misuse of information and communication technologies in sovereign territory, not damaging critical infrastructure, protecting critical infrastructure, taking steps to ensure supply chain security, and not interfering with emergency response teams. Despite this significant milestone, issues remain, including the lack of accountability.

States are constantly engaging in cyber operations to achieve their national objectives. However, some states exert more restraint than others, with checks and balances in place at the national and international level placing guardrails around their cyber operations—as the United Kingdom has described it, "responsible cyber power."[103] However, this results in a situation where there is a group of states who are less restrained in their cyber operations (e.g., Russia, China, and Iran), posing significant threats to other states that comply with regulatory frameworks and exercise restraint (e.g., the United Kingdom and the United States).[104] The United States and its allies have made efforts to hold state actors to account for their cyber operations which has manifested in the form of attribution. There are numerous cases of attribution of state actors for hacking attempts and commercial espionage.[105] However, attribution does not appear to deter states from behaving badly. Stronger forms of accountability and consequences need to be developed so that there are consequences for states that do not uphold international norms, which in turn could collectively enhance international cybersecurity.

WHAT PROTECTIONS FOR VOLUNTEERS?

Ukraine's cyber defense has relied on hundreds of thousands of IT volunteers who have supported cyber operations against the Russian state, but it is not clear to whether they are afforded any protection under international law. According to the International Committee of the Red Cross, examples of participation in hostilities include activities that "directly cause harm to another party, either directly inflicting death, injury or destruction, or by directly harming the enemy's military operations or capacity . . . interfering electronically with military computer networks and transmitting tactical targeting intelligence for a specific attack."[106] It is unclear to what extent a cyber operation conducted by a civilian—based in Ukraine or beyond—on Russia's government, propaganda apparatus, and industrial base would qualify as direct participation, or whether volunteers are covered by international norms as non-state actors.[107] For example, hackers geographically based in some territories, such as the United States or the United Kingdom, joining Ukrainian cyberattacks, could be breaking national law.[108] The involvement of volunteer cyber forces from different geographies thus presents new challenges for international norms and laws designed with states in mind.

CONCLUSION

There are significant ramifications from the conflict in Ukraine for the global cybersecurity community. Significant investment in defense is essential to ensure cyber resilience in the face of evolving threats. While this was clear before Russia's invasion, it was not obvious that Ukraine's cyber defense would be as effective

as it has been so far. What is clear in Ukraine's case is that the near-decade of having to defend its national interest in cyberspace—which necessitated collaboration across government and with the whole of Ukrainian society, combined with working with allies and the private sector—has resulted in its strong cyber defense to date. Investing in cyber defense, preparing for hybrid warfare, prioritizing information security, and fostering a culture of cyber awareness throughout society has enhanced its resilience and ability to withstand Russia's cyber and information campaigns.

Russia will likely remain an acute and persistent threat for many countries in the Western alliance. Therefore, there is a lot that can and should be learned from Ukraine's experience so far to put cyber defenders on a stronger footing in the face of adversarial threats in cyberspace. Significant questions still remain around whether or not this varied and novel alliance between allies, volunteers, and the private sector in cyberspace can be replicated in another scenario. But what all will note from the Ukrainian case so far is that a good defense is perhaps just as effective as a good offense.

From Script Kiddies to Cyber Warriors

The Private Lines of Defense in the Ukraine Conflict

BY: MELANIE GARSON

Introduction

From the early days of the Ukraine conflict, pundits globally awaited the first "cyber war." Building on assumptions of the evolution of warfare in the digital age and Russia's consistent gray zone cyber activity in Ukraine since 2014, governments and security analysts were anticipating the accompanying cyber "bomb," and they quickly began to puzzle over the lack of a clear cyber front. Many of these questions stemmed from a fundamental misunderstanding of the complexity of offensive cyber activity, as well as of its limitations in delivering widespread guaranteed impacts in the same way as kinetic activity. However, one year on, the State Service of Special Communication and Information Protection of Ukraine (SSCIIP) reports that cyberattacks on Ukraine continue to escalate from their pre-Christmas levels, with a particular focus on public institutions and civil infrastructure. [109] Global cyber activity has reached some of the highest levels ever observed, heavily concentrated on Ukraine; however, due to the continued efforts of a new collective cyber defense alliance, their ability to further Russia's kinetic activity has been limited.

The unlikely combination of tech companies, tech platforms, tech workers, hobbyists, and hacktivists that helped Ukraine working alongside governments and international organizations has mounted "arguably the most effective cyber defense in history."[110] By ensuring that the internet infrastructure is secure and operational, that internet services are accessible, and that information is available and not weaponized, these non-state actors were able to rapidly alter Russia's military communications strategy. This new cyber defense alliance continues to be able to thwart Russia's cyber ambitions to impact critical communications pathways and has materially contributed to tipping the balance of power in the conflict.

Whilst the rapid integration of these disparate cyber actors at the core of Ukraine's wartime cyber command can provide many lessons for states in their approach to a more holistic and cooperative cyber defense, the strategy

opens up a new set of risks. Bringing in civil society and commercial actors into active cyber combat puts pressure on key laws and norms, including the blurring of defensive and offensive cyber activity and the extent that this legitimizes non-state actors as parties to the conflict–and, by extension, places them as well as states as legitimate targets for retaliation.

This paper explores the role of these new defenders of the digital sphere and draws on the discussions of the roundtable held with representatives of the platforms, infrastructure and content distribution networks, and civil society actors as to provide recommendations for building clarity into the engagement with tech companies and non-state cyber defenders and disrupters when these are thrust onto the frontline of cyber defense. [111]

The Never-Ending Consolidated Threat Surface

Russia's vision of offensive cyber sits within a wider approach of "information confrontation" or "information warfare" that encompasses both the network attacks that are at the basis of most Western conceptions of offensive cyber activity and the information operations that usually sit within the U.S. definition of cognitive warfare.[112] This has been reflected in Russian Defence Ministry statements clearly defining a strategy of disruption to both the physical network infrastructure and the information space in order to degrade the societal fabric of an opponent.[113] Compounded by the rise of drone warfare and the multi-domain battlefield, the control of a stable internet source is a key element of strategic success.[114]

With this conception of cyber, defense must span multiple physical and digital threat surfaces, from the information layer through to the backbone of the internet infrastructure, most of which are out of the control of states. Tech companies are now diversified throughout the internet stack, from the information layer, down through the hardware and device layer, into essential services and access control, and all the way to the backbone infrastructure. Meta owns more kilometers of subsea cables than British Telecom, and Starlink's mega-constellation of LEO satellites far outpaces that of the United Kingdom and the United States, with 3,236 satellites currently operational.[115]

Simultaneously, the communications infrastructure is being consolidated, with a few companies being able to provide services throughout the internet stack.

Major Providers: Communications Infrastructure

	Amazon	Alphabet	Meta	Microsoft
Platform	Amazon Shopping	Google search BardAI	Facebook, Instagram, Whatsapp	Windows App, Bing, Azure OpenAI
Hardware & Devices	Echo, Ring, smart home products	Chromebook, Pixel, Google Home	Portal, Quest headset	Microsoft Surface
Internet Services & Access	Amazon Web Services (AWS) CloudFront	Google Cloud	Facebook Wi-Fi	Azure, Cybersecurity services
Infrastructure	Satellite internet service (Project Kuiper). AWS subsea cables	Google Fiber subsea cables	2 Africa subsea cable partners	Investment in subsea cables, data centers

Source: Pete Furlong and Melanie Garson, *Disrupters and Defenders: What the Ukraine War Has Taught Us About the Power of Global Tech Companies* (London: Tony Blair Institute for Global Change, 2022), https://www.institute.global/insights/geopolitics-and-security/disrupters-and-defenders-what-ukraine-war-has-taught-us-about-power-global-tech-companies.

This consolidation has increased throughout 2022 and into 2023, as companies have added to their assets at all levels of the communications infrastructure. Elon Musk's purchase of Twitter in October 2022 added a platform to the Space X family, Google Cloud's acquisition of Mandiant increased its cloud security, and Microsoft's investment into OpenAI suggests that the trend towards developing representation throughout the internet stack as well as control over new and emerging tech is set to continue. [116]

With vast amounts of the core communication infrastructure now sitting in the hands of commercial companies, the ability and agility to materially interfere with Russia's multi-level cyber and information warfare could not be achieved without the active and willing cooperation of tech companies.

The Front Line of Commercial Cyber Power

Before the tanks had rolled into Ukraine, many of the large tech companies had already started shoring up Ukraine's cyber defenses alongside governments and the NATO Cooperative Cyber Defence Centre for Excellence, most notably Microsoft's detection of the Foxblade malware attack on February 23, 2022.[117] This marked the escalation of both high-profile and more subtle commercial cyber power taking on the defense of Ukraine and limiting Russia's actions across the physical and digital components of the communications ecosystem, as well as supporting the dissemination of life-saving real time information and applications for Ukrainians. Russia found itself up against the brightest cyber minds as well as the collective might of the global cyber community.

Building Resilient Internet Infrastructure

The internet "backbone"—the wires, pipes, and servers that keep it operational—is notoriously fragile to both environmental events and deliberate interference. Regaining operational function once it is damaged can often be challenging, such as in Tonga which suffered nearly five weeks of internet outage after its subsea cable was damaged in a volcanic eruption. Similarly, the recent Cyclone Gabrielle in New Zealand and the earthquake in Turkey left vast areas with limited connectivity.

In Ukraine, human internet traffic dropped as much as 33 percent in the days immediately after the invasion.[118] This was driven by Russia's encroachment on the routing of data—leaving parts of Ukraine reliant on Russian cables and subject to Russia's restrictions and limitations—such as the Viasat KA-SAT attack that impacted routers in Ukraine and consistent physical degradation to fiber optic cables and electrical power facilities from targeted bombings.[119] Through the strategic destruction of over 4,000 mobile base stations, thousands of kilometers of fiber optic cable, and 18 Ukrainian radio broadcast towers, Russia has prevented local residents from sharing information or receiving information on humanitarian corridors.[120] Russia also keeps its own soldiers in a media blackout so they cannot question their actions. As Russia physically occupies cities, it also occupies the digital ecosystem, with internet traffic rerouted from Ukrainian networks to Russian ones and Ukrainian internet service providers threatened with the loss of their communication equipment unless they join the Russian networks.[121] A parallel more resilient and operational internet became critical to Ukraine's ability to counter the Russian offensive.

Starlink's rapid response to Mykhailo Fedorov's tweet that saw 500 terminals on the ground in Ukraine

within five days, 25 of which were transmitting data within a week, has now been widely confirmed as being determinative in ensuring military and civilian communications.[122] Between mid-March and December 2022, Starlink traffic in Ukraine increased by 1,600 percent.[123] Highly resilient and able to withstand electronic jamming attacks more adeptly than previously anticipated, Starlink's shoring up of Ukraine's internet infrastructure has been the lynchpin of basic battlefield communications, from weapons supply arrivals to its more controversial use in drone warfare.

In parallel, internet backbone carriers were withdrawing their service provision in Russia. By March 7, 2022, Cogent and Lumen—two of the world's largest internet service providers, who had provided transit for Russia's key national fiber backbone operators including Rostelcom and Transtelcom, its key mobile phone operators, and Russia's search engine Yandex—stopped providing services. Driven by the possibility that the networks could be used as part of Russia's offensive cyber activity and concern for its employees, with downstream impacts felt as far as Kazakhstan, Tajikistan, Uzbekistan, Belarus, and Iran, this exit left Russia with the challenge of finding alternative infrastructure provisions to enable its strategic internal and external cyber operations. [124]

Embedding Internet Security

Activities on the Ukraine-Russia cyber front had been bubbling since 2016. However, the increase of malicious cyber activity in the months prior to the physical invasion provided governments and tech companies opportunities to secure the digital domain more effectively than the physical battlefield. The CyberPeace Institute has tracked over 1,408 cyberattacks and operations from across 87 different threat actors related to the Ukraine conflict, and whilst these numbers are significant, they likely still do not capture the full picture of the cybersecurity threat.[125] Cloudflare has reported that in March 2022 application layer attacks in Ukraine rose by 1,300 percent and that between February 2022 and February 2023 an average of 10 percent of all traffic to Ukraine was mitigations of potential attacks. At its high point on October 29, 2022, 39 percent of total traffic to Cloudflare's Ukrainian customer websites was DDoS attack traffic.[126]

As previously noted, Microsoft's Threat Intelligence Centre (MSTIC) had been working closely with Ukraine's government and was able to mitigate the "Foxblade" wiper software on 19 government and critical infrastructure entities across the Ukraine government on the day before the war started. It continued to provide support, identifying and protecting against numerous destructive cyberattacks on nearly 50 Ukrainian agencies and entities as well as over 128 targets including government agencies and nongovernmental agencies in 42 countries.[127] Similarly, Cisco Talos was working closely with the government of Ukraine to respond to the WhisperGate malware in January 2022 and translated their responses into protections for customers across Ukraine.[128] Other companies, such as ESET and Recorded Future, have provided key services, tools, and threat intelligence. Google has also reported its role in countering the 250 percent increase in phishing attacks targeting Ukraine and 300 percent increase targeting NATO countries (as compared to 2020), as well as more destructive attacks in Ukraine than in the previous eight years.[129]

Both Microsoft and AWS were pivotal in securing Ukraine's public sector infrastructure by facilitating the transfer of its data from physical data centers to the cloud within 10 weeks of the Ukraine government passing an urgent amendment to its data protection law on February 17, 2022, to allow data to be held externally. Microsoft provided $107 million of technology services to facilitate this transition.[130] Ukraine's deputy prime minister and minister of digital transformation, Mykhailo Fedorov, highlighted the contribution of AWS in migrating key public registers and records to the cloud as "one of the biggest contributions to Ukrainian victory."[131]

And while large companies like Google have provided cybersecurity protections for over 150 humanitarian organizations from DDoS attacks through its Project Shield, smaller companies essential to the cybersecurity ecosystem have also thrown their weight into the collective defense of Ukraine's internet. Cloudflare has been providing internet availability monitoring services to Ukraine's government, moving secure encryption key data for customers out of at-risk data centers in Ukraine, Russia, and Belarus, and providing free protections for Ukrainian organizations under its Project Galileo. Romanian company BitDefender offered a year's worth of free cybersecurity assistance to business, government, and private citizens of Ukraine. Similarly, California based Vector AI offered its services free of charge for targets or organizations under attack, and companies such as SentinelOne, Avast, and CrowdStrike offered services or decryptors for free.[132]

Ensuring Internet Accessibility

The number of companies controlling the distribution of content (content distribution networks or CDNs) is very small and critical in facilitating internet accessibility. Companies with a very small market share can have a large impact on access to the internet and companies such as Cloudflare—with 80 percent of market share—are in a key position to keep the internet accessible.[133] The role of internet accessibility in countering Russia's cyber offense is more nuanced than that of ensuring security, as it requires managing compliance with sanctions alongside providing access to the internet to balance Russia's information warfare. While companies such as Fastly, alongside a number of other web companies, quickly ceased working with Russian-based companies altogether, other CDNs stopped paid services to comply with international sanctions but continued to provide free services. Cloudflare, which had been threatened with Russian shutdowns previously, has taken the position that Russia would celebrate their closure if they were to exit and opted to continue providing free, open, private, and secure internet services to the Russian people to counter Russia's attempts to raise a digital iron curtain.[134]

Similarly, Virtual Private Network (VPN) providers have continued to counter Russian attempts to separate from the rest of the internet by providing avenues for Russians to stay connected to international media sources. VPN use in Russia reached a peak demand of 2,692 percent above average on March 14, 2022. as access to the open internet became constricted. Canada's Windscribe publicly committed to providing an extra 30GB of data freely to both sides of the conflict, ensuring that Russians have access to the open internet. ProtonVPN waived all fees from Russian customers on the basis of a "strong moral obligation" to be there and ensure the Russian people have freedom of access to the internet.[135]

Secure Hardware for Hard War

The communications hardware and the apps that run on it have also become key determinants in the offense-defense balance. Access to personal communication devices has become key, both for soldiers on the battlefield and civilian threat alerts.[136] Affordable hardware is required for the internet, but the sanctions regime has restricted most providers including Apple, Samsung, Lenovo, HP, AMD, Dell, and Intel from operating in Russia and selling the semiconductors, computers, phones, and server hardware that form the physical end point of the communications system. This also impacts the dual-use hardware that enables critical technologies, such as unmanned drones. Ukraine can rely on diversified sources of communications hardware to enable sophisticated battlefield technologies; however, Russia is buying communications hardware, such as electronic jammers, on Chinese-owned AliExpress.[137] This access to diversified supply of trustworthy and secure hardware, in order to both operate and process the information gathered from drones, has reshaped Ukraine's ability to continually resist Russia.

Defending the Information Frontier

With Russia's cyber strategy heavily rooted in the battle for control of the information domain, it is at this level that tech companies have had to fight some of their hardest battles. Russia's physical digital occupation strategy—restricting internet access through physical means, such as by rerouting networks—has been accompanied by an equally draconian censorship strategy both inside Russia and in occupied parts of Ukraine. While Russia's media law punishing "fake news"—which was passed in the early days of the conflict—led to most media companies and platforms being forced to leave Russia, its physical occupation in parts of Ukraine have left Ukrainians without key information sources including Instagram, YouTube, and the messaging app Viber.[138] Google's search engine was disabled in Donetsk, Luhansk, and Kherson on the claim that it was advocating violence and terrorism against Russians, and Russia claimed to have shut Twitter, Instagram, and YouTube in parts of Zaporizhzhia.[139]

The role of tech platforms in balancing information flows and countering Russia's massive influence operations capacity became critical for both strategic and humanitarian reasons even before the kinetic offensive began. Early signs of the Russian invasion were spotted by open-source researchers monitoring traffic data on Google Maps, requiring Google to disable it in order to protect Ukrainian citizens from detection.[140] And as Russian state-owned media became the driving force of disseminating false content about the invasion, platforms such as Meta, Reddit, TikTok, Alphabet (the parent company of Google and YouTube), Microsoft, Spotify, and Telegram restricted access to RT and Sputnik news in Europe—and in some cases globally—and their apps were banned from app stores. Adobe prevented Russian government-controlled media organizations from accessing its creative and document cloud services to avoid being complicit in the creation of harmful information. Google, YouTube, Twitter, and Meta restricted Russian state-based entities from being able to monetize ads on their platforms, and companies including Snapchat and the Japanese-based company Viber implemented wider bans on displaying ads across their apps. Search engines including DuckDuckGo, Google, and Bing downranked links associated with Russian disinformation. Even Chinese platforms such as Douyin, Weibo, WeChat, and Bilibili undertook a process of blocking accounts spreading information that could put Chinese students in Ukraine at risk.[141]

In order to counterbalance Russia's information offensive and recognizing the strategic and humanitarian imperative to secure access to information, commercial tech companies across the ecosystem were quick to facilitate alternative access to information, both for Ukrainians and Russians. Google disrupted over 1,950 instances of Russian information operation on its platforms in 2022, including claims that Ukraine operates biolaboratories for generating biological weapons and information operations linked to destructive malware attacks.[142] Microsoft's Russian Propaganda Index run by its AI for Good Lab also recorded significant increases in traffic to Russian propaganda websites from January 2022, with a rise of 216 percent in the last week of February 2022.[143] Through identifying the scope of the disinformation globally, tech companies enabled governments, companies, and other organizations to implement counter-responses and neutralize the disinformation strategies. Google's Trust & Safety team has disabled accounts associated with coordinated information operations, including the disruption of YouTube channels, blogs, and AdSense accounts, and has removed domains from Google News surfaces.

Tech companies have also sought to balance this by providing alternate sources for legitimate information to the Russian people. Twitter launched a parallel site on the dark web alongside its shadow-banning of Russian government accounts. Media outlets have taken advantage of the increased Telegram use to create new sources of news distribution, and Microsoft's Skype extended free communication in and out of Ukraine. Cumulatively, these rapid and far-reaching actions have restrained the impact of Russia's digital information blockade, as a strategic tool to facilitate both the active conflict and its supporting actions.

Private Companies in the Trenches

Behind the tech companies, however, there is another cadre of private actors and companies in the trenches of the cyber elements of the conflict. The cyber defense ecosystem also relies on a complex web of ethical hackers, or "cybersecurity researchers," who report vulnerabilities to companies and governments. Prior to the conflict, ethical hacking was illegal in Ukraine, with fines for those found detecting bugs in state computers. In early February 2022, however, in the face of mounting cyberattacks, the Ukraine government committed to decriminalize bug bounties to allow for better detection of security vulnerabilities.[144] At the outset of the war, homegrown cybersecurity companies such as Cyber Unit Technologies approached the government to offer their help, forming the basis of Mykhailo Fedorov's 150,000–200,000-strong IT Army.[145] Hacken.io, the Kyiv-based bug bounty platform, also launched a "Cyber Army" to encourage security researchers on its platform to search for vulnerabilities in Russian websites to be used by the government.[146] Similarly, the Estonia-based bug bounty platform HackenProof invited disclosure of critical vulnerabilities in both Ukrainian and Russian infrastructure, with commitment to disclose them to the Ukrainian authorities for both defensive and offensive use.[147] U.S.-based cybersecurity research companies such as HackerOne, in compliance with the sanction regimes, were able to continue facilitating bounty payments to Ukrainian cybersecurity researchers after resolving some technical difficulties, but they paused payments to researchers in Belarus and Russia.

Challenges of Private Cyber Defenders in Geopolitical Crises

Whilst the response of tech companies to defend across the cyber ecosystem has been unprecedented and contributed significantly to Ukraine's success to date, it has not been without challenges. The limited exposure of tech companies to engagement at this level has led at times to a lack of appreciation of the complexity of their actions, as well as a lack of consistency and coherence across policies. From diplomacy by Twitter to navigating sanctions regimes, political pressure, and the negative impacts of rapid decisionmaking, the lack of experience that private cyber defenders have in navigating geopolitical crises has led to conflicting actions that could at times undermine internet resilience and fail at countering Russia's offensive cyber operations.

Moving Fast and Breaking Things

The rapid action of tech companies in the early days of the crisis reflects an agility that can be valuable to tip the balance of power in a conflict. Whether responding to political and corporate pressure from the outpouring of support for Ukraine, a need to protect employees, fear of sanctions, Russia's "fake news law," a genuine demonstration of disapproval, or in some cases even to increase their public relations value, companies moved fast and were far-reaching in their actions. Whilst this may have had measurable impacts at the time, it may also not have offered sufficient time to consider the full ramifications of their actions for long-term cyber stability. This at times has led to backtracking or possibly undermining avenues to counter Russia's cyber operations.

The sanctions regime threatened the right of Russians to have universal connectivity and left the Russian people more at risk of government information control strategies, as well as threatening the basic nature of the open, globally connected, secure and trustworthy internet. After significant lobbying by Access Now and the Wikimedia Foundation, in April 2022 the U.S. government issued an advisory providing exemptions for companies providing internet services, recognizing the need to keep information flows accessible to people in Russia and Belarus.[148] However, this came too late for key companies such as Lumen and Cogent Communications, who had already withdrawn their services from Russia, partly due to unclear policy. At the other end of the spectrum, the bug bounty platform HackerOne found itself disabling payments to Ukrainian

cybersecurity researchers whilst they sought to amend their systems to comply with the sanctions regimes.[149] This prevented them from providing crucial support to Ukrainian researchers—as well as access to knowledge of key vulnerabilities at a critical time, potentially.

While some companies tried to move slower to strike a more balanced position between supporting Ukraine and preserving the integrity of the internet and access to information for Russians, they found themselves under greater pressure from public calls from Ukraine's government and consequent stakeholder pressures rather than that of their own governments. In Myanmar, civil society organizations urged Telenor to stay in place as an alternative might be complicit with the regime, thereby worsening the situation. Navigating this level of geopolitical foresight is out of the scope of normal operating procedure for many companies and opens the question of how home governments can shield companies that may have to make unpopular decisions for long-term cybersecurity and internet stability.

Finding Coherence to Complexity

The Ukraine conflict has highlighted the challenge for commercial companies to find coherence and consistency when navigating information warfare in the heat of complex geopolitical crises. While companies may have acted quickly, this has sometimes been inconsistent with previous actions or policies and has required them to backtrack on their actions. Meta was challenged by inconsistencies within their own content moderation policies when evidence emerged that they had provided a temporary change to their hate-speech policies to allow calls for violence against Russians and Russian soldiers, including Russian president Vladimir Putin and Belarusian president Alexander Lukashenko.[150] They then had to revise, limit, and reverse decisions in the face of accusations from Russia that they were fueling hate against the Russian people.[151]

Social media platforms also found themselves caught in a dilemma when placed in the position of being the evidence repository of war crimes that could be crucial for future criminal tribunals, particularly with how this may intersect with their own terms of service preventing illegal and harmful content. Furthermore, Twitter's turn to international humanitarian law as the basis of banning tweets showing images of prisoners of war highlighted not only the potential that private companies could be considered parties to the conflict but the lack of clear internal or external guidelines for commercial actors' decisionmaking in complex geopolitical crises. Tech companies also found themselves caught in balancing public disclosures of their support, having to tread carefully between protecting employees, following corporate principles, and ensuring that their information does not provide strategic advantages for Russia—decisions outside of the norms of its responsibility.

Companies reported that legal counsel was not always nuanced, making it hard for many to carry out a holistic assessment of the wider geopolitical implications of their actions and manage the competing priorities inherent to the cyber dimensions of the conflict. Key to this challenge is that companies are used to assessing risks through a financial lens, rather than through societal priorities or by seeking to reduce their liabilities. For a company that deals with encryption standards, an exit from Russia may be a reduction of liability; but with a long-term geopolitical focus on cyber stability, if that company is replaced by a Russian equivalent, the cyber ecosystem may be more insecure. If cyber stability is going to depend on the controllers of the communications infrastructure being able to navigate through the complexity of both cyber-enabled and cyber-dependent warfare, then new mechanisms are going to be required in order to guarantee greater coherence in times of crises. This includes greater understanding of the decisionmaking procedures that

companies undertake in addressing their involvement in geopolitical crises, as well as mechanisms to provide companies with the foundational understanding of the impact of discrete actions through the internet stack—such as withdrawal of service—on geopolitical conflict.

Wavering Clarity and Commitment

As tech companies responded both independently and under overt and covert political pressure to counteract Russia's deliberate strategy of cutting or destabilizing internet access, they could not predict the level of long-term commitment this would entail. This has led to tech companies wavering in their commitments and trying to limit the use of their infrastructure provisions, possibly creating greater instability. Starlink—despite its importance to Ukraine's defense, with over 150,000 Ukrainians using it daily to access the internet by May 2022, and its role in enabling surveillance and reconnaissance aerial vehicles and unmanned aerial vehicles—threatened to stop funding the program and asked the Pentagon to take over the costs.[152] Although a large proportion of terminal and internet use costs were being covered by the U.S. Agency for International Development (USAID) and other partners, Starlink was seeking further support.[153] Further, SpaceX has restricted the use of Starlink for drones, highlighting that the support was intended for humanitarian purposes but not to be weaponized—possibly putting Ukraine at greater risk, both through the action itself and through the public declaration of their position.[154]

In November 2022, Microsoft pledged a further $100 million to Ukraine's digital alliance, promising that Ukraine would be able to use Microsoft's cloud and data centers in Europe throughout 2023. While the continued support is generous, as Microsoft chairman Brad Smith stated at the Munich Security Conference in February 2023, it is a "one year at a time" approach.[155] This stands in contrast to state positions, such as the U.S. promise to stand by Ukraine "for as long as it takes."[156] Questions arise as to the dangers of dependency on critical infrastructure or cybersecurity support that can be withdrawn on a whim or under corporate pressures and obligations to shareholders.

Cyber Defenders as Legitimate Targets

While Microsoft has been clear that its support in the Ukraine conflict is entirely defensive, as any offensive action would violate its pledge made as a part of the Cybersecurity Tech Accord, from a legal standpoint commercial tech companies may find themselves technically participants to the conflict and thus legitimate targets for attack, particularly with the lines between consumer and military tech becoming more blurred and many militaries relying on consumer tech for military.[157] Even the most sophisticated companies might not anticipate this, with Starlink's restriction on the use of its terminals for offensive purposes reflecting that they hadn't fully anticipated this possibility. This would turn quite closely on the nexus between the private company's action and the consequent military action, or whether the data held in a private cloud was military data.[158] The recent attempt by Ukraine to draft a law to legalize its volunteer IT army into part of its cyber command may help to mitigate the ambiguity for some individual security researchers.[159] However, companies may still remain exposed. Actions such as that of Hacken.io's "Cyber Army," in which the intention to hand vulnerabilities to the Ukrainian authorities is clearly stated, could be construed as voluntary participation in hostilities—and thus open the possibility of a private company becoming a legitimate target in retaliation.[160]

PREPARING FOR THE NEXT CYBER-ENABLED CRISIS

In an era of increasing converging crises, the risks exposed by the Ukraine war are not fading. Ukraine

benefited from strong Western support, both politically and in the public sphere, making the case for tech company action relatively clear. In other contexts, it may not be so straightforward. Tech companies have struggled to balance their engagement in more complex crises such as ones in Myanmar and Ethiopia, and the closure of international offices as part of the tech downturn—such as that of Twitter's only African office—could leave them ill-prepared to address future global challenges. It is also still not clear how companies will fully address the crisis-inducing potential of generative AI systems and similar emerging technologies that could be exploited in misinformation campaigns by reducing the barrier to generating synthetic media, deepfakes, and malicious content.

The conflict in Ukraine has highlighted the challenges and dangers to cyber stability of trying to formulate sensitive policies under pressure, along with the urgent need for tech companies to be able to assess the impact of their individual and cumulative actions in a crisis or in post-crisis stabilization and reconstruction. New mechanisms are needed, similar to Environmental, Social and Governance (ESG) frameworks or Covid-19 protocols, that embed geopolitical risk considerations into the corporate governance of those companies responsible for the cyber ecosystem, in order to ensure coherence and consistency across geopolitical crises. Companies should also seek to embed tech geopolitics experts who see beyond liability into more holistic geopolitical impacts in their decisionmaking procedures, as well as civil society organizations that can provide more nuanced pictures of situations in a country.

At the same time, governments and the international community need to rethink their interactions with big tech to ensure that they are providing sufficient support for companies to balance their actions with the core principles and norms of the liberal and democratic world order. The role of the company in the internet stack often determines its level of interaction across the cyber ecosystem. Tech companies have highlighted the need for neutral convenors to assist in helping align action without it appearing like big tech collusion or strong-arming. Newer agreements and partnerships, such as the Declaration for the Future of the Internet and the Freedom Online Coalition, have been formulated with these kinds of issues in mind but have struggled to gain influence and traction.

Internet stability is at the heart of the multi-domain era of warfare. As militaries invest in increasingly interconnected and intelligent weaponry, access to stable, resilient, and secure communications is crucial. And as offensive strategies expand from the depths of the sea to potential interference in interplanetary networking, the range of actors required to defend these domains far expand the capabilities of most militaries alone. Cyber power will belong to those states that create the mechanisms to ensure the coherence, consistency, transparency, reliability, and geopolitical responsibility of those private actors currently defending the cyber front lines of the Ukraine conflict.

Facing the Cyber State Threat

A Strategic Approach

BY: AMY ERTAN

Introduction

In 2002, the NATO formally acknowledged the need to defend against cyber threats.[161] Over the following two decades, cyber defense was institutionalized and understood as a core part of national defense, by both allies and the alliance.[162] As an example, since 2016, NATO allies have recognized cyberspace as a domain of operations in which NATO must defend itself as effectively as it does in the air, on land, and at sea. At the national level, the majority of states have evolved their position on cyber defense through the development of national strategies, the establishment of national authorities responsible for defending against cyber threats, and a range of additional initiatives designed to deter, detect, defend against, and respond to malicious cyber activity.[163]

These developments are intrinsically linked with changes in the increasingly complex cyber threat landscape. Now more than ever, adversarial states have shown a willingness and capability to use cyber operations to support their strategic objectives. As a result, cyberspace now plays a key role in strategic competition.

As NATO's 2022 Strategic Concept explains, "Malign actors seek to degrade our critical infrastructure, interfere with our government services, extract intelligence, steal intellectual property and impede our military activities."[164] For that reason, though recognizing that nations must defend themselves against the full breadth of cyber threats, this paper specifically focuses on state-sponsored threat actors, who attempt to use cyberspace to undermine their target's national security to further their own strategic and military objectives.[165]

The war in Ukraine, for example, has highlighted Russia's willingness to leverage cyber operations in the run-up to–and during–the invasion, against Ukraine and others.[166] Russia has used cyber operations to

support a range of strategic objectives in Ukraine, from destructive malware to disrupt and degrade the activities of the Ukrainian government and military to attacks on civilian infrastructure—including critical national infrastructure—to undermine public confidence and trust in the Ukrainian government.[167] The uptick in Russian state-sponsored activity against Ukraine in the months leading up to and including the start of the invasion also showed that the attackers were maximizing their access to data and systems to support intelligence gathering, stealing or leaking sensitive information to further their narratives.[168] Some public reports reveal the targeting of state and non-state actors through cyber operations and kinetic military strikes simultaneously, though it remains unclear if these were coordinated.[169]

Beyond those involved in Ukraine, there are a number of state and state-sponsored actors that pose a threat to NATO allies and like-minded states. The United Kingdom has highlighted that China and Russia pose the greatest threat to its national security due to evidence of their sophisticated cyber capabilities, followed by Iran and North Korea.[170] Disruption due to malicious cyber activity has been felt recently across and beyond the alliance.[171] These include a significant disruption from major cyberattacks against Albania's national information infrastructure in mid-2022, which Albania and other nations have publicly attributed to Iran.[172] More recently, in March 2023, North Macedonia hosted a NATO senior stakeholder visit concerning its ongoing experience defending against hybrid attacks, including cyberattacks.[173] Beyond the significant loss of communications in Ukraine, a major cyberattack against private satellite provider Viasat in February 2022 was reported to have caused disruptions across Europe, far beyond Ukraine's borders.[174] Throughout 2022, multiple industry research reports have highlighted an increase in malicious cyber activity on users across NATO countries and have linked the activity to several state-sponsored threat actors, largely under the direction of Russian government agencies as well as China-sponsored cyber actors.[175] Nor has Russian malicious cyber activity been limited solely to targets in Ukraine. According to Google, phishing attacks against users in NATO countries from Russian government-sponsored cyber threat actors increased by 300 percent in 2022 compared to 2020.[176] These cyber campaigns are aimed at a broad range of targets, from government and critical infrastructure to private sector organizations and citizens.

So far, malicious activity in cyberspace against NATO has been assessed as falling below the level of armed conflict. Researchers focusing on cyber defense and national security nonetheless face a conceptual challenge: while "cyber warfare" appears to set the bar too high, given that most cyber operations are below the threshold of war, it is also inaccurate to say that current activity in cyberspace represents a "peaceful" state. Experts have presented conceptual models to understand the current nature of cyberspace, speaking of a state of "un-peace," or attempting to understand cyber operations within the strategic studies lenses of "sub-threshold" or "gray zone" warfare.[177] In essence, the message for policymakers, as well as senior political and military leaders, is clear: there is no peace in cyberspace.

The consensus at NATO is that, as stated firmly in the 2022 Strategic Concept, "Cyberspace is contested at all times."[178] It is no longer exceptional that states, including NATO members, face disruption to their critical infrastructure due to malicious cyber activity.[179] Reflecting on recent cyberattacks against Ukraine, research by the Economic Security Council of Ukraine argues that the opportunistic use of cyberspace to seek strategic advantages is not expected to change any time soon.[180] Instead, increasing aggression in cyberspace is the "new normal," and in the context of growing instability internationally, this has several key implications for cyber defenders.

Recognizing this new escalated baseline for state-sponsored cyber activity against NATO and like-minded countries, including Ukraine, this paper reflects on the current cyber threat landscape to consider how NATO allies and like-minded states may effectively defend themselves in this new normal. With a particular focus

on the strategic landscape, the paper attends to the need for dynamic strategic positioning for cyber defense, national and international resilience-building efforts, and sustainable engagement with relevant industry actors in peacetime, crisis, and conflict.

A Comprehensive Strategic Approach to Cyberspace

Beyond Ukraine, attacks on NATO nations add to the growing body of evidence that cyberspace is always contested. Russia "seeks to establish spheres of influence and direct control through coercion, subversion, aggression and annexation," using "conventional, cyber and hybrid means against us [NATO members] and our [their] partners."[181] It is not alone. The People's Republic of China (PRC) "strives to subvert the rules-based international order, including in the space, cyber and maritime domains," using "malicious hybrid and cyber operations and its confrontational rhetoric and disinformation to target Allies and harm Alliance security."[182] More generally, growing geopolitical instability over the past year has brought security to the forefront of state agendas around the world and prompted a revisiting of assumptions around national security and defense postures. Cyber defense must be considered within this reckoning, reflecting how the cyber threat landscape has evolved.

Defending the rules-based international order requires a cohesive strategic vision, and states cannot go this alone. Broadly speaking, democratic states must not loosen their commitment to the rules-based order—they must instead, as the 2023 Munich Security Conference report reflected, do more to ensure a stable proposal to make this order work for a greater number of states that may otherwise be attracted to Russia and China's attempts at revisionism.[183] In the cyber domain, there is an equal need to agree on how democratic states can continue to cooperate to develop norms for responsible state behavior in cyberspace, address issues of cyber deterrence, and raise the cost of malicious cyber activity against them. The 2023 U.S. Cybersecurity Strategy outlines an ambitious national agenda for cyberspace that will only be strengthened by sustainable partnerships and the effective use of international organizations, such as NATO, to form a coherent international approach to adversarial state threats.[184] Consensus commitment to using international frameworks to address strategic international threats in cyberspace, whether at the NATO alliance level or beyond, provides a level of collective strength that exceeds any individual state's efforts to challenge the contested geopolitical landscape.

More specifically, the increasing ease with which authoritarian states use malicious cyber activity to undermine the current rules-based international order requires a commitment from NATO allies and like-minded states to refuse to tolerate this "new normal" and impose painful consequences in response to these escalating levels of malicious cyber activity. This includes a refusal to accept the normalization of state-sponsored malicious cyber activity against critical infrastructure. Democratic states can steer a proactive course by explicitly noting recent escalation in cyberspace and refusing to be complacent to this new, raised baseline of more frequent and disruptive cyberattacks by adversarial state-sponsored actors. This will involve renewing their pledge to a norms-based approach to cyberspace, embracing a dynamic approach to develop new policies and impose costs in line with the evolving cyber threat landscapes, and not sacrificing any commitment to the principles of responsible state behavior in cyberspace, even as adversaries attempt to shirk them in attempt to gain offensive advantages. Any alternative course risks being perpetually on the back foot, handing the initiative to authoritarian states for them to shape cyberspace to their advantage.

Various international organizations can help facilitate this shift in vision to different degrees, including but not limited to the NATO, the European Union, the United Nations, and the Organization for Security and Cooperation in Europe (OSCE). NATO has made it clear that a single or cumulative set of malicious cyber

activities may reach a level of an armed attack, at which point NATO's North Atlantic Council may invoke Article 5 of the North Atlantic Treaty.[185] This decision is to be taken on a case-by-case basis. Yet for this threshold of "armed attack" to be meaningful, it is essential to have a clear understanding of baseline activity. This means being proactive and refusing to become, as one NATO colleague puts it, a "boiling frog"—referring to an analogy in which a frog in a pot does not realize its worsening situation if the water around it comes to a boil gradually. States must ensure that they do not unwittingly build a tolerance to escalated activity, thus prompting future escalation. Therefore, to prevent adversarial actors subtly raising the threshold of acceptable malicious cyber behavior, states must both deliver on their rhetoric to hold responsible threat actors accountable and double down on resilience to decrease the success of subsequent malicious cyber campaigns.

The decades-long debate on how deterrence applies in cyberspace has highlighted the complexities of feasibly and consistently holding adversaries accountable.[186] It has become clear that NATO deterrence in cyberspace is underpinned by the ability to deliver meaningful consequences to malicious cyber threat actors.[187] Norms work if they are upheld; states thus require the ability to impose costs on others who intentionally seek to undermine them. The discourse on international norms in cyberspace reveals a contested and complex environment in which in which many nations may have different positions.[188] Still, NATO allies have made it clear in a 2022 statement that NATO is "ready to impose costs on those who harm us [its members] in cyberspace."[189] It also pledged to revise the alliance's deterrence and defense posture, including in cyberspace.[190] The successful application of these principles will call for action from beyond the NATO alliance.

Such a stance not only requires a vision that plans for a variety of future threat landscapes but one that also enables collaboration between states and international organizations to develop a comprehensive answer to cyber defense and deterrence. Within NATO, a coherent allied approach on how cyber contributes to overall deterrence and defense will lay out the consequences of malicious activity in cyberspace to malign state actors. This signaling, in addition to existing diplomatic and economic tools such as joint cyber attribution or responses in other non-cyber domains, shows that allies can be dynamic and act firmly where norms continue to be challenged by states.

At the national level, relevant stakeholders and decisionmakers across defense communities must understand the nature of cyberspace and the challenges surrounding cyber deterrence concepts. Crucially, they must also understand that the pace and scale of cyberattacks are unlikely to slow down unless actions are taken to adapt and respond proactively. While cyber defenders might feel they are constantly firefighting attempted cyberattacks, failing to make time to elaborate a strategic vision to respond to these attacks risks "missing the forest for the trees" and remaining stuck in a reactive posture in which the firefighting will never cease—and may in fact increase. Without a consistent conceptual approach to cyber deterrence, accompanied by adherence to a comprehensive strategic vision both nationally and internationally, states remain disadvantaged when adversarial states appear to act unpredictably. Strategic thinking also needs to include, and take place on, a supra-national level.

Remodeling Cyber Resilience

Growing instability across the international landscape has prompted a refocus on cyber defense and resilience as an integral part of national defense. Resilience in this context refers to society's ability to resist and recover from shocks and combines both civil preparedness and military capability; cyber resilience extends this state to systems relying on cyber resources.[191] There is a growing recognition that governments need greater insight into their cyber resilience posture across the entire national ecosystem, including across the private sector and

especially relating to critical infrastructure.[192] In line with a forward-looking strategic vision, a strong cyber resilience posture has been recognized as essential to deter, detect, and prevent malicious cyber activity. Many states have set out their intended plans to enhance their cyber resilience, either as part of a cyber defense strategy or within broader national security doctrine.[193]

Resilience forms a core part of NATO's founding principles, in which Article 3 outlines the responsibility of allies to "maintain and develop their individual and collective capacity to resist armed attack" via "self-help and mutual aid."[194] For cyber defense specifically, NATO encourages nations to strengthen their defensive posture in cyberspace through three mechanisms: the NATO Defence Planning Process, which includes cyber-related capability targets for allies over a four-year cycle; the Cyber Defence Pledge, whereby since 2016 allies have committed to enhancing their cyber defenses with a focus on seven key objectives; and more broadly, the support of each NATO nation's seven baseline requirements for national resilience.[195]

As mentioned above, many NATO allies have already articulated their cyber defense vision. However, resilience is a continuous and iterative process, and as states face the escalating security situation in the Euro-Atlantic area, their momentum must not falter. Not only must states work to overcome persistent challenges facing capability building relating to cyber defense, but they must also adapt to the threat landscape considering activity in and beyond Ukraine.

Regarding the former, some challenges are systemic and experienced by the majority of states to some degree, when it comes to strengthening their cyber defense and resilience posture. Limited investment, a shortfall in the skilled cyber workforce (particularly in the public sector and the defense forces), organizational resistance to change, legacy systems, and disengaged leaders can all lead to stagnancy in maturing a state's cyber defense and resilience posture.[196] To address and overcome barriers to greater cyber defense and preparedness, states must be able to track progress and react whenever they risk falling short of delivering their strategic visions. This requires top-level leadership across government and defense forces, a framework for effective civil-military cooperation—particularly in the high-level transition from peacetime to crisis or conflict—and a consideration of how cyber activity on critical infrastructure may impact military mobility. Enhancing resilience and situational awareness means tackling systemic challenges relating to information-sharing at the national level and between allies. Further, in recent years greater attention has been given to the importance of a healthy national ecosystem of cybersecurity industry actors who can swiftly offer support in a crisis and who are resilient themselves.

Effective resilience also means taking a comprehensive approach to cyber defense, which includes tackling challenges in new ways. For example, while many states have now released plans addressing the education of a cyber workforce, there is room for improvement. Few states have a defined strategy for the retention of cyber expertise within the public sector, where they risk losing experts to competitive industry packages, and few states have published a declarative perspective on how they are approaching recruitment of cyber experts for the public sector or the military. For all states, there is a great deal of opportunity to explore in hiring through targeting diversity of all kinds, whether based on gender, career stage (e.g., attracting mid-career talent from other sectors into cyber defense), or discipline (e.g., attracting economists or psychologists into the field). This example of recruitment is one of many in which adjusting to the modern defense environment requires a gear-change in tactics, and states must continue to look forward to acting proactively and decisively.

Looking at current events, Ukraine has shown a significant amount about cyber resilience in times of conflict. Significant commentary has focused on the fact that the large-scale cyber campaigns leveraged against Ukraine have had little apparent success.[197] The foremost reason for this is often credited to Ukraine's cyber resilience,

much of which had been actively developed in response to previous Russian aggression against Ukraine, particularly from 2014 onwards.[198] Cyber capacity-building measures appear to have contributed substantively to Ukraine's resilience, and in turn, the war in Ukraine has prompted states to reflect on cyber defense within broader resilience and crisis management response plans. There are opportunities across the board to strengthen preparedness for a cyber crisis, whether it is by ensuring that there is a cyber crisis response plan or by including cyber in national crisis response frameworks. Such plans should be comprehensive, involving stakeholders across the public and private sectors, with regular exercising to maximize readiness in case of crisis.

A related view on Ukraine's impressive cyber resilience posture heralds the significant assistance Ukraine received from the United States and others since 2014, which allowed it to decrease its reliance on insecure software and implement many of the cyber defenses that protected it against of Russia's activity in cyberspace. Outside of armed conflict, the principle of assistance to allies remains much the same and is increasingly relevant beyond formal NATO structures. Ukraine showed allies how critical it is that where a state needs help to protect itself against an aggressor, it gets the support required. Certainly, within the NATO alliance, the principle of resilience follows the adage "a rising tide lifts all ships"; as the relatively more vulnerable states mature their national resilience to malicious cyber activity, the alliance becomes more resilient overall.

Beyond current commitments, NATO members and like-minded states must be empowered to highlight the best use of capacity-building measures, perhaps by using national cyber maturity assessments (or similar) to check where a state is not meeting minimum baseline levels of security or where they are not making progress over time. The use of a metric-driven approach to cyber resilience—taking care to choose appropriate metrics, of course—would enable states to check their progress over time and to highlight where they are struggling with progress and may need assistance, such as the sharing of best practices, from allies.

Furthermore, events in Ukraine and beyond have highlighted the need for effective assistance coordination mechanisms, which could be activated in response to significant malicious cyber activity. Currently, there are no comprehensive frameworks for effectively coordinating cyber assistance in a crisis. Ukraine highlighted this need for a coordinator to swiftly prioritize needs and allocate tasks to a range of public and private actors offering bilateral assistance. Such a framework would need to think about how the receiver prioritizes its most urgent needs in a cyber crisis (or a crisis with cyber aspects); articulates these needs to potential helpers; deconflicts offers of assistance from various actors; arranges the logistics of assistance, including physical movement and access to technology; and deconflicts any issues relating to legal constraints or privileges and immunities, ensuring those offering support in a crisis are legally protected should their actions inadvertently cause damage, in "Good Samaritan" fashion. Therefore, in taking a comprehensive approach, national cyber crisis frameworks and response plans should consider how states could offer, but also receive, cyber assistance from outside actors, including other states and industry providers. Using NATO as a platform, allied states are working to operationalize these activities through the development of a virtual cyber incident support capability, which will operate on a voluntary basis and use national assets.[199]

The final aspect, once an effective resilience plan is in place that accounts for all aspects of cyber defense and crisis management, is to ensure that it works in practice via a comprehensive and holistic approach to exercising and training, including national and international cyber exercises as well as meaningful integration of cyber into joint exercises. These exercises, when mimicking a national crisis, benefit from drawing in stakeholders across military and civil communities as well as from a range of relevant national actors, such as critical infrastructure operators and the cybersecurity industry providers that would likely be engaged

in a real-world cyber crisis. While care is needed to avoid duplication against existing exercises or training fatigue where a limited set of skilled expertise is constantly refreshed instead of conducting business as usual, exercising should be leveraged to ensure preparedness across a range of aspects.[200]

Sustainable Resilience and Private Sector Engagement

Any analysis of Ukraine's cyber defense activities through 2022 would be incomplete without analyzing the critical role of industry actors, many of whom donated (among other things) licenses, software packages, and infrastructural services. In the immediate run-up to, and early stages of, the invasion in February 2022, Ukraine rapidly ingested a range of private sector and bilateral state assistance in cyberspace.[201] Actors from the private sector proved instrumental in helping Ukraine react rapidly and defend against cyber threats through the provision of cyber threat intelligence[202], cloud data storage[203], and a range of cyber defense products including denial of service mitigation services, incident response capabilities, and security software licenses.[204] In the information space, for telecommunications and broader support of digital infrastructure, Starlink's satellite terminals have been critical in maintaining communications by the Ukrainian military and civilian authorities.[205] Private sector support for Ukraine's cyber defense efforts has played a significant role in reshaping the conflict.[206] This has been so significant that it has been recognized by the Ukrainian government, to the extent that in May 2022, Google received the first Peace Prize from Ukraine in recognition of the company's support, which included a significant cybersecurity assistance package.[207]

This aspect of direct private sector involvement has prompted a more urgent approach to private-public engagements, with the United States among those claiming to have increased collaboration with industry partners on cybersecurity issues as a direct result of activity in Ukraine.[208] Increased private sector participation, alongside the cyberattack against Viasat, also prompted discussions around private sector actors' place in a conflict, such when they may be considered legitimate military targets in cyberspace.[209] More broadly, there is an emerging and increasing concern around private sector dependencies and the sustainability of private sector engagement in a crisis, particularly in cases where states may be reliant on industry providers to provide or operate critical infrastructure support.[210] Nowhere is this illustrated more neatly than in the case of SpaceX's Starlink, a satellite internet service that has been essential in maintaining connectivity for critical services in Ukraine—and the Ukrainian military—since February 2022. When SpaceX announced it was no longer planning to offer the satellites or licenses to Ukraine without cost—having already spent almost $100 million supporting Ukrainian's internet service—it prompted a scramble in which other actors came forward to sponsor ongoing service delivery.[211] During a dramatic series of public exchanges in autumn, SpaceX highlighted that the company could not "indefinitely" fund Starlink connectivity in Ukraine.[212] While service availability was eventually maintained with external assistance, the loss of these services, which Ukraine has become reliant on during the conflict, could have been devastating to Ukraine's war effort.[213]

While Starlink may be an extreme example, with few competitors in the market of portable satellite communications technology, the war highlights the sheer number and breadth of actors now enmeshed in the provision of rapid cyber assistance to a state in conflict. Private sector actors cannot afford to give products for free or below cost indefinitely. Ultimately, shareholders have a say, and as more organizations announce their inability to donate services, the limits of this type of ad hoc free support will likely be revealed over time. While Microsoft has announced its support free of charge until the end of 2023, for example, the Telegraph reported that the company likely faced some business impact as a result, turning down new cloud clients in mid-2023 due to capacity constraints.[214]

While private-public cooperation for cyber defense is by no means a novel topic for governments, there is no agreed current market model for private sector actors to sustainably provide cyber assistance in the context of a conflict or where receiving actors cannot necessarily cover the costs involved. Much like the required coherent strategic vision for cyber deterrence discussed in an earlier section, the United Kingdom and its allies will have to face the challenge of market sustainability soon as they look towards Ukraine and beyond. Acknowledging the evolving cyber threat landscape in which we expect governments to continually face cyber crises in the future, stakeholders need market incentives to ensure that they do not end up continually rallying in an ad hoc manner, as in the case of Starlink in Ukraine.[215]

There are two kinds of incentives to encourage private sector actors to provide support to states who may not have the resources to pay them directly. First, encouraging donations through the perspective of norms and in support of democratic values. This admittedly relies on a moral incentive targeting the values and strategic positioning of service provider—but it can be encouraged. When announcing continued support for Ukraine free of charge through 2023, Microsoft referenced their support of "international stability and the protection of fundamental rights across Europe and around the world."[216] Recognizing that for-profit organizations have different overarching goals from government defense stakeholders, there is nonetheless a path forward for defense stakeholders to harness and shape the way industry increasingly engages with norms.[217] Second, coordinating alternative funding mechanisms that might include ad hoc bilateral assistance from other states. This may involve the creation of an emergency or sustained funding mechanism through which states with greater resources can contribute funds to shore up a state's cyber defenses, in line with the international resilience-building measures discussed above.

A focus exclusively on the first option—appealing to private sector non-financial motivations—is unlikely to succeed in the long term. For the latter option, it is not yet clear what kind of body or group of states might coordinate such a fund, or if this fund is politically feasible given the expectation of future attacks. A sustainable approach will need to include both kinds of incentive to work for everyone involved and ensure adequate market participation in the long term. This is a market challenge greater than any one nation; it will require states to come together to determine an appropriate framework for engagement. Any framework, in addition to accounting for sustainable provision of services in terms of funding, must also clarify the roles and authorities where private sector organizations provide digital or cyber defense services to ensure seamless integration into national defense. In spring 2023, SpaceX acted to restrict the Ukrainian military's use of Starlink connectivity for drone control, claiming that the organization's technology was being weaponized by Ukraine in a way not originally intended and at odds with its terms and conditions of service.[218] While private organizations must retain the right to provide their services as they wish, unexpected changes to the service provision mid-conflict are not, putting it lightly, an effective way to engage and build a commercial relationship. Mechanisms coordinating private sector assistance, in times of cyber crisis and broader conflict, must set out clear frameworks for engagement at the start to avoid such ad hoc surprises.

Again, the driving force for any framework would be to take an active approach to the coordination of assistance. This means setting structures in place so that when nations need to request external industry support during a major cyber incident, mechanisms to arrange this support already exist and can be agile while also accounting for sustainable deployment and maintenance.

Conclusion

The current strategic landscape demonstrates that cyberspace continues to be fertile ground for pushing the boundaries of conflict and raising the level of malicious activity against states beyond what is considered

acceptable in the rules-based international order. Cyberspace is increasingly used by state-sponsored actors to conduct malicious cyber activity, where they can achieve asymmetric effects while maintaining plausible deniability and provocatively challenge the rules-based order championed by NATO and like-minded nations.

This contested cyberspace is well on the way to becoming the "new normal," with a baseline that has incrementally increased over time to the levels of pervasive disruption seen today. State-sponsored cyber operations against critical infrastructure are happening more frequently, and nations must take a proactive stance on cyber's role in defense. States defending the norms-based order cannot be complacent nor unaware of the "boiling frog" scenario; they must not subconsciously adjust to this new baseline of malicious cyber activity and they must resist becoming more tolerant of their adversaries' disruptive actions. Instead, policymakers and political leaders must unite at a strategic and political level to present a strategic vision for the rules-based order. For cyberspace, this strategic vision must address deterrence in cyberspace and intolerance to adversarial activity. Second, resilience must remain a priority, particularly for all states struggling to make progress on systemic challenges including resources, capacity-building, and funding. Enhancing resilience means helping all those on whom one depends for overall security. Learning from Ukraine, resilience must also include the ability to adapt quickly in a crisis, with the ability to receive and deliver cyber assistance as required. Finally, there is a future in which cybersecurity providers to Ukraine all withdraw their donated support due to their capacity constraints in a market economy, and this would be hugely disruptive to Ukrainian cyber defense capabilities. The international community needs a model for sustainable private sector provision of assistance—not just for Ukraine, but to be employed in principle wherever a state needs emergency assistance and has funding constraints. The best time to have created such a framework would have been before facing the risks of over-reliance on the private sector in the middle of a difficult conflict. The second-best time is now.

The contents of this paper do not represent the official views of NATO. All views are the author's own.

About the Editors and Authors

James A. Lewis writes on technology and public policy at the Center for Strategic and International Studies (CSIS), where he is a senior vice president, holds the Pritzker Chair, and directs the Strategic Technologies Program. Before joining CSIS, he was a diplomat and a member of the Senior Executive Service with extensive negotiating, politico-military, and regulatory experience. Lewis developed ground-breaking policies on satellite remote sensing, encryption, high-tech exports to China, and cybersecurity. He led the first U.S. delegation to the Wassenaar Arrangement Experts Group. Lewis was the rapporteur for three UN Groups of Governmental Experts on Information Security and an adviser to the first Open Ended Working Group. His work on how norms and confidence-building measures build stability is foundational for international cybersecurity. Lewis has authored numerous publications since coming to CSIS, is frequently quoted in the media, and has testified numerous times before Congress. He leads a long-running Track 2 dialogue with the China Institutes of Contemporary International Relations. He received his PhD from the University of Chicago.

Georgia Wood is the program manager and research associate for the CSIS Strategic Technologies Program. In this role, she manages the Strategic Technologies Program and conducts research on cybersecurity, emerging technologies, digital innovation and transformation, and digital governance. Previously, she was a digital communications intern for the United Nations Foundation, a counterintelligence digital communications intern for the Office of the Director of National Intelligence (ODNI), a research assistant for the University of Michigan Institute for Healthcare Policy and Innovation, and an external relations intern at CSIS. She holds a BA in international studies with a focus on international security, norms, and cooperation from the University of Michigan.

Amy Ertan is a cyber and hybrid policy officer at NATO Headquarters where she supports the development of cyber policies and initiatives across the alliance. Previously she was a researcher at the NATO Cooperative Cyber Defence Centre of Excellence, a visiting fellow with the Hague Program on International Cyber Security, and a cybersecurity fellow at Harvard's Belfer Center for Science and International Affairs. Amy received her

PhD in information security from Royal Holloway University of London, and her research on cyber strategy and emerging security challenges have led to publications on topics including national cyber capabilities, military exercising, offensive cyber operations and cyber risk management. She has CISSP and CRTIA qualifications and has previously worked in private sector roles in cyber intelligence, cyber exercise design, and human factors cybersecurity research.

Melanie Garson is the cyber policy lead and acting director of geopolitics at the Tony Blair Institute for Global Change. Her work focuses on cyber policy, the geopolitics of the internet, the rise of tech companies as geopolitical actors, data governance as well as the intersection of emerging tech, foreign policy and diplomacy. She is also an associate professor in international conflict resolution & international security in the Department of Political Science at University College London where she teaches about new and emerging technologies and the future of conflict in the digital age. She also teaches courses on international negotiation and tech diplomacy. Melanie presents regularly at international conferences in Europe, the Middle East and Africa on the implications of cyber, AI and emerging technologies on geopolitics and foreign policy, as well as provides commentary at major media outlets including BBC, Sky, CNN, France 24, and Deutsche Welle.

Melanie is an accredited mediator and has worked as a solicitor in the International Disputes department of Freshfields Bruckhaus Deringer. She received her PhD from University College London and holds a Master of Arts in Law and Diplomacy from the Fletcher School.

Erica Lonergan (nee Borghard) is an assistant professor in the Army Cyber Institute at West Point. She is also a research scholar in the Saltzman Institute of War and Peace Studies at Columbia University. Prior to that, she held positions as a senior fellow at the Carnegie Endowment for International Peace and the Atlantic Council. Previously, Erica served as a senior director on the U.S. Cyberspace Solarium Commission. Erica also held an appointment as a Council on Foreign Relations International Affairs Fellow, with placement at JPMorgan Chase and U.S. Cyber Command, and has served as an assistant professor and executive director of the Rupert H. Johnson Grand Strategy Program in the Department of Social Sciences at West Point. Erica received her PhD in political science from Columbia University. Her book, *Escalation Dynamics in Cyberspace*, coauthored with Shawn Lonergan, was recently published with Oxford University Press.

Julia Voo is a cyber fellow at Harvard's Belfer Center where she leads the team behind Harvard Belfer's National Cyber Power Index. She was formerly the research director for the China Cyber Policy Initiative. Her other areas of research concern geopolitics, technical standards, and the Digital Silk Road. A 2019 graduate of Harvard Kennedy School's Master in Public Administration program, Julia served earlier at the British Embassy in Beijing where she covered China's cyber and AI policy from a commercial perspective, technical standards, and other trade policy issues. She lived in Beijing for seven years with stints at the EU Delegation to China, Carnegie-Tsinghua Centre for Global Policy, and she has spent time at the UK Cabinet Office. Julia is currently also the director of cyber and tech policy at HP Inc. Julia's research, writings and commentary have featured in several media outlets including the *Financial Times*, the *Economist*, BBC World News, *Wired* Magazine, and Cyberscoop.

Endnotes

1 Joseph Marks, "Here's what cyber pros are watching in the Ukraine conflict," Washington Post, February 24, 2022, https://www.washingtonpost.com/politics/2022/02/24/heres-what-cyber-pros-are-watching-ukraine-conflict/; Kier Giles, "Putin does not need to invade Ukraine to get his way," Chatham House, December 21, 2021, https://www.chathamhouse.org/2021/12/putin-does-not-need-invade-ukraine-get-his-way; and Maggie Miller, "Russian invasion of Ukraine could redefine cyber warfare," *Politico*, January 28, 2022, https://www.politico.com/news/2022/01/28/russia-cyber-army-ukraine-00003051.

2 Gavin Wilde, *Cyber Operations in Ukraine: Russia's Unmet Expectations* (Washington, DC: Carnegie Endowment for International Peace, December, 2022), https://carnegieendowment.org/2022/12/12/cyber-operations-in-ukraine-russia-s-unmet-expectations-pub-88607; Lennart Maschmeyer and Nadiya Kostyuk,"There Is No Cyber 'Shock And Awe': Plausible Threats In The Ukrainian Conflict," War on the Rocks, February 8, 2022, https://warontherocks.com/2022/02/there-is-no-cyber-shock-and-awe-plausible-threats-in-the-ukrainian-conflict/.

3 "Brace for Russian cyber attacks as Ukraine crisis deepens, Britain says," Reuters, January 28, 2022, https://www.reuters.com/world/europe/brace-russian-cyber-attacks-over-ukraine-britain-says-2022-01-28/; and Dan Sabbagh, "UK firms warned of Russian cyberwar 'spillover' from Ukraine," *The Guardian*, February 23, 2022, https://www.theguardian.com/technology/2022/feb/23/uk-firms-warned-russia-cyberwar-spillover-ukraine-critical-infrastructure.

4 Garrett Graff, "The US Watches Warily for Russia-Ukraine Tensions to Spill Over," *Wired*, February 15, 2022, https://www.wired.com/story/russia-ukraine-cyberattacks-spillover/.

5 Erica D. Lonergan, "The Cyber-Escalation Fallacy: What the War in Ukraine Reveals About State-Backed Hacking," *Foreign Affairs*, April 15, 2022, https://www.foreignaffairs.com/articles/russian-federation/2022-04-15/cyber-escalation-fallacy.

6 YourAnonNews (@YourAnonNews), "#Anonymous is currently involved in operations against the

Russian Federation. Our operations are targeting the Russian government. There is an inevitability that the private sector will most likely be affected too. While this account cannot claim to speak for the whole (con)," Twitter post, February 24, 2022, 4:04 p.m., https://twitter.com/YourAnonNews/status/1496954233492541444.

7 Jai Vijayan, "Inside Killnet: Pro-Russia Hacktivist Group's Support and Influence Grows," Dark Reading, February 1, 2023, https://www.darkreading.com/ics-ot/killnet-pro-russia-hacktivist-group-support-influence-grows.

8 Lorenzo Franceschi-Bicchierai, "Inside Ukraine's Decentralized Cyber Army," Vice, July 19, 2022, https://www.vice.com/en/article/y3pvmm/inside-ukraines-decentralized-cyber-army.

9 Erica D. Borghard and Shawn W. Lonergan, "The Logic of Coercion in Cyberspace," *Security Studies* 26, no. 3 (2017): 452–81; and Maggie Smith, Erica D. Lonergan, and Nick Starck, "What Impact, if Any, Does Killnet Have?" Lawfare, October 21, 2022, https://www.lawfareblog.com/what-impact-if-any-does-killnet-have.

10 David Vergun, "Partnering With Ukraine on Cybersecurity Paid Off, Leaders Say," U.S. Department of Defense, December 3, 2022, https://www.defense.gov/News/News-Stories/Article/Article/3235376/partnering-with-ukraine-on-cybersecurity-paid-off-leaders-say/.

11 Erica D. Borghard and Shawn W. Lonergan, "Can States Calculate the Risks of Using Cyber Proxies?" Orbis 60, no. 3 (Summer 2016): 395–416; and Tim Maurer, *Cyber Mercenaries: The State, Hackers, and Power* (Cambridge: Cambridge University Press, 2018).

12 Janne Hakala and Jazlyn Melnychuk, *Russia's Strategy in Cyberspace* (Riga, Latvia: NATO Strategic Communications Centre of Excellence, June 2021), 5, https://stratcomcoe.org/publications/russias-strategy-in-cyberspace/210.

13 Justin Sherman, "Untangling the Russian web: Spies, proxies, and spectrums of Russian cyber behavior," Atlantic Council, September 19, 2022, https://www.atlanticcouncil.org/in-depth-research-reports/issue-brief/untangling-the-russian-web/.

14 David Sanger and Nicole Perlroth, "Pipeline Attack Yields Urgent Lessons About U.S. Cybersecurity," *New York Times*, May 14, 2021, https://www.nytimes.com/2021/05/14/us/politics/pipeline-hack.html; and "Meat giant JBS pays $11m in ransom to resolve cyber-attack," BBC, June 10, 2021, https://www.bbc.com/news/business-57423008.

15 "REvil ransomware gang arrested in Russia," BBC, January 14, 2022, https://www.bbc.com/news/technology-59998925.

16 Andreas Hagen, "The Russo-Georgian War of 2008," in Jason Healey, ed., *A Fierce Domain: Conflict in Cyberspace, 1986 to 2012* (Vienna, VA: Cyber Conflict Studies Association, 2013); and Jeffrey Carr, *Inside Cyber Warfare: Mapping the Cyber Underworld* (Sebastopol, CA: O'Reilly Media, 2012).

17 Tim Maurer, "Cyber Proxies and the Crisis in Ukraine," in *Cyber War in Perspective: Russian Aggression Against Ukraine* (Tallinn, Estonia: NATO CCD COE Publications, 2015); and Nadiya Kostyuk and Yuri M. Zhukov, "Invisible Digital Front: Can Cyber Attacks Shape Battlefield Events?" *Journal of Conflict Resolution* 63, no. 2 (2019): 317–47.

18 Mark Clayton, "Ukraine election narrowly avoided 'wanton destruction' from hackers," *Christian Science Monitor*, June 17, 2014, https://www.csmonitor.com/World/Passcode/2014/0617/Ukraine-election-narrowly-avoided-wanton-destruction-from-hackers.

19 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/.

20 Olena Goncharova, "Cyber warrior steps up effort to help in war with Russia," *Kyiv Post*, February 10, 2015, https://archive.kyivpost.com/article/content/war-against-ukraine/cyber-warrior-steps-up-effort-to-help-in-war-with-russia-380184.html.

21 Erica D. Lonergan and Shawn W. Lonergan, "Cyber Operations, Accommodative Signaling, and the De-Escalation of International Crises," *Security Studies* 31, no. 1 (2022): 32–64.

22 Politically motivated cyber proxies, in particular, have historically proliferated in the context of other enduring rivalries, such as India and Pakistan or China and its neighbors in East Asia.

23 Andy Greenberg, *Sandworm: A New Era of Cyberwar and the Hunt for the Kremlin's Most Dangerous Hackers* (New York: Doubleday, 2019).

24 Jon Bateman, *Russia's Wartime Cyber Operations in Ukraine: Military Impacts, Influences, and Implications* (Washington, DC: Carnegie Endowment for International Peace, December 2022), https://carnegieendowment.org/2022/12/16/russia-s-wartime-cyber-operations-in-ukraine-military-impacts-influences-and-implications-pub-88657.

25 Andy Greenberg, "Russia's Sandworm Hackers Attempted a Third Blackout in Ukraine," *Wired*, April 12, 2022, https://www.wired.com/story/sandworm-russia-ukraine-blackout-gru/; and Sean Atkins, "A web of partnerships: Ukraine, operational collaboration, and effective national defense in cyberspace," Atlantic Council, August 30, 2022, https://www.atlanticcouncil.org/content-series/airpower-after-ukraine/a-web-of-partnerships-ukraine-operational-collaboration-and-effective-national-defense-in-cyberspace/.

26 Daryna Antoniuk, "Ukraine's state-owned nuclear power operator said Russian hackers attacked website," The Record, August 17, 2022, https://therecord.media/ukraines-state-owned-nuclear-power-operator-said-russian-hackers-attacked-website/; and "Ukraine Nuclear Operator Reports Cyberattack on Its Website," The Defense Post, August 17, 2022, https://www.thedefensepost.com/2022/08/17/ukraine-nuclear-operator-cyberattack/.

27 Sean Lyngaas, "Russian hackers allegedly target Ukraine's biggest private energy firm," CNN, July 5, 2022, https://www.cnn.com/2022/07/01/politics/russia-ukraine-dtek-hack/index.html.

28 DTEK Group (@dtek_en), "The russian federation has carried out a #cyber attack on #DTEKGroup's #IT infrastructure. ¼," Twitter post, July 1, 2022, 10:54 a.m., https://twitter.com/dtek_en/status/1542884325015830528?s=20&t=o_Qz2y72EVvYBC8gAHDLMQ; and Bateman, *Russia's Wartime Cyber Operations in Ukraine*.

29 Antoaneta Roussi, "Meet Killnet, Russia's hacking patriots plaguing Europe," *Politico*, September 9, 2022, https://www.politico.eu/article/meet-killnet-russias-hacking-patriots-plaguing-europe/.

30 Alexander Heid, "KillNet Utilizes CC-Attack: A Quick & Dirty DDoS Method," SecurityScorecard, May 25, 2022, https://securityscorecard.com/blog/killnet-utilizes-cc-attack-a-quick-dirty-ddos-method.

31 Microsoft, *Defending Ukraine: Early Lessons from the Cyber War* (Redmond, WA: Microsoft, June 2022), https://query.prod.cms.rt.microsoft.com/cms/api/am/binary/RE50KOK.

32 Jonathan Greig, "CISA says Killnet DDoS attacks on U.S. hospitals had little effect," The Record, February 7, 2023, https://therecord.media/ddos-hospitals-cisa-killnet-limited-effects/.

33 American Hospital Association, "HHS alerts health sector to pro-Russian hacktivist threat," News release, January 30, 2023, https://www.aha.org/news/headline/2023-01-30-hhs-alerts-health-sector-pro-russian-hacktivist-threat.

34 Daryna Antoniuk, "Pro-Kremlin hackers target Latvia's parliament after declaring Russia a sponsor of terrorism," The Record, August 10, 2022, https://therecord.media/pro-kremlin-hackers-target-latvias-

parliament-after-declaring-russia-a-sponsor-of-terrorism.

35 WE ARE KILLNET, Telegram post, October 10, 2022, 1:34 p.m., https://t.me/killnet_reservs/3019.

36 WE ARE KILLNET, Telegram channel, accessed April 27, 2023, https://t.me/s/killnet_reservs.

37 Jai Vijayan, "Inside Killnet: Pro-Russia Hacktivist Group's Support and Influence Grows," Dark Reading, February 1, 2023, https://www.darkreading.com/ics-ot/killnet-pro-russia-hacktivist-group-support-influence-grows.

38 Daniel Smith, "Exploring Killnet's Social Circles," Radware Blog, January 27, 2023, https://blog.radware.com/security/threat-intelligence/2023/01/exploring-killnets-social-circles/.

39 "Самые опасные хакеры мира I" [World's Most Dangerous Hacker], VK Video, September 22, 2022, https://vk.com/video/@tvduma?z=video-160662967_456251570%2F6266e70c032a050f43.

40 Lonergan and Lonergan, "Cyber Operations, Accommodative Signaling, and the De-Escalation of International Crises."

41 Franceschi-Bicchierai, "Inside Ukraine's Decentralized Cyber Army," and Matt Burgess, "Ukraine's Volunteer 'IT Army' Is Hacking in Uncharted Territory," *Wired,* February 27, 2022, https://www.wired.com/story/ukraine-it-army-russia-war-cyberattacks-ddos/; and Stefan Soesanto, *The IT Army of Ukraine: Structure, Tasking, and Ecosystem* (Zurich: Center for Security Studies June 2022), 6, https://css.ethz.ch/content/dam/ethz/special-interest/gess/cis/center-for-securities-studies/pdfs/Cyber-Reports-2022-06-IT-Army-of-Ukraine.pdf.

42 Shaun Waterman, "Ukraine Scrambles to Draft Cyber Law, Legalizing Its Volunteer Hacker Army," *Newsweek*, March 14, 2023, https://www.newsweek.com/ukraine-drafting-new-law-legalizing-volunteer-hacker-cyber-army-red-cross-1786814.

43 Erica Lonergan, "Cyber Proxies in the Ukraine Conflict: Implications for International Norms," Council on Foreign Relations Blog, March 21, 2022, https://www.cfr.org/blog/cyber-proxies-ukraine-conflict-implications-international-norms

44 Shaun Waterman, "Ukraine's Volunteer Cyber Army Could Be Blueprint for the World: Experts," *Newsweek*, February 21, 2023, https://www.newsweek.com/ukraine-war-cyber-army-attack-strategy-warfare-1780970.

45 Burgess, "Ukraine's Volunteer 'IT Army' Is Hacking in Uncharted Territory."

46 Soesanto, *The IT Army of Ukraine: Structure, Tasking, and Ecosystem*, 6. However, it is important to note that the Estonian cyber unit is focused on defensive efforts and is more clearly organized and controlled by the Estonian government.

47 Chris Stokel-Walker and Dan Milmo, "'It's the right thing to do': the 300,000 volunteer hackers coming together to fight Russia," *The Guardian,* March 15, 2022, https://www.theguardian.com/world/2022/mar/15/volunteer-hackers-fight-russia; and IT ARMY of Ukraine Telegram channel, accessed May 16, 2023, https://t.me/s itarmyofukraine2022?before=1250.

48 Ibid., 4.

49 Waterman, "Ukraine's Volunteer Cyber Army Could Be Blueprint for the World: Experts."

50 Soesanto, *The IT Army of Ukraine: Structure, Tasking, and Ecosystem*, 11-13.

51 IT ARMY of Ukraine, Telegram post, February 26, 2022, 10:50 a.m., https://t.me/s/itarmyofukraine2022/1.

52 Lonergan, "Cyber Proxies in the Ukraine Conflict: Implications for International Norms.".

53 Jason Healey, "The Spectrum of National Responsibility for Cyberattacks," *The Brown Journal of World Affairs* 18, no. 1 (2011), https://www.jstor.org/stable/24590776?seq=1#metadata_info_tab_contents.

54 Open-ended working group on developments in the field of information and telecommunications in the context of international security, *Final Substantive Report* (New York: United Nations, March 10, 2021), https://front.un-arm.org/wp-content/uploads/2021/03/Final-report-A-AC.290-2021-CRP.2.pdf.

55 Jason Healey and Olivia Grinberg, "'Patriotic Hacking' Is No Exception," Lawfare, September 27, 2022, https://www.lawfareblog.com/patriotic-hacking-no-exception.

56 Peter Pascucci and Kurt Sanger, "Cyber Norms in the Context of Armed Conflict," Lawfare, November 16, 2022, https://www.lawfareblog.com/cyber-norms-context-armed-conflict.

57 Vladimir Soldatkin and Humeyra Pamuk, "Biden tells Putin certain cyberattacks should be 'off-limits'," Reuters, June 16, 2021, https://www.reuters.com/technology/biden-tells-putin-certain-cyber-attacks-should-be-off-limits-2021-06-16/.

58 Julian Barnes, "U.S. Military Has Acted Against Ransomware Groups, General Acknowledges," *New York Times*, December 5, 2021, https://www.nytimes.com/2021/12/05/us/politics/us-military-ransomware-cyber-command.html.

59 "NATO prepares for cyber war," *Politico*, December 6, 2022, https://www.politico.com/news/2022/12/03/nato-future-cyber-war-00072060; and North Atlantic Treaty Organization, "Keynote Address by NATO Secretary General Jens Stoltenberg at the NATO Cyber Defence Pledge Conference in Italy," Speech transcript, November 10, 2022, https://www.nato.int/cps/en/natohq/opinions_208925.htm.

60 "Conti ransomware group announces support of Russia, threatens retaliatory attacks," CyberScoop, February 25, 2022, https://cyberscoop.com/conti-ransomware-russia-ukraine-critical-infrastructure/.

61 "Conti Ransomware: The History Behind One of the World's Most Aggressive RaaS Groups," Flashpoint, October 4, 2022, https://flashpoint.io/blog/history-of-conti-ransomware/.

62 Monica Pitrelli, "Leaked documents show notorious ransomware group has an HR department, performance reviews and an 'employee of the month'," CNBC, April 13, 2022, https://www.cnbc.com/2022/04/14/conti-ransomware-leak-shows-group-operates-like-normal-tech-company.html. "To Be CONTInued? Conti Ransomware Heavy Leaks," Cyberint, March 9, 2022, https://cyberint.com/blog/research/contileaks/.

63 Silvia Amaro, "The U.S. has warned on China's support for Russia. Now the EU says 'we need to remain vigilant,'" CNBC, March 3, 2023, https://www.cnbc.com/2023/03/03/us-warns-about-china-support-to-russia-europe-says-we-need-to-remain-vigilant.html; and Ashley J. Tellis, "'What Is In Our Interest': India and the Ukraine War," Carnegie Endowment for International Peace, April 25, 2022, https://carnegieendowment.org/2022/04/25/what-is-in-our-interest-india-and-ukraine-war-pub-86961.

64 Sean T. Lawson, *Cybersecurity Discourse in the United States: Cyber-Doom Rhetoric and Beyond* (New York: Routledge, 2020).

65 Waterman, "Ukraine Scrambles to Draft Cyber Law, Legalizing Its Volunteer Hacker Army."

66 Kadri Kaska, Anna-Maria Osula, and LTC Jan Stinissen, *The Cyber Defence Unit of the Estonian Defence League: Legal, Policy and Organisational Analysis* (Tallinn, Estonia: NATO Cooperative Cyber Defense Centre of Excellence, 2013), https://ccdcoe.org/library/publications/the-cyber-defence-unit-of-the-estonian-defence-league-legal-policy-and-organisational-analysis/.

67 Shane Huntley, "Fog of war: how the Ukraine conflict transformed the cyber threat landscape," Google Threat Analysis Group Blog, February 16, 2023, https://blog.google/threat-analysis-group/fog-of-war-how-the-ukraine-conflict-transformed-the-cyber-threat-landscape/; and Insikt Group, *Themes and Failures of Russia's War Against Ukraine* (Recorded Future, February 2023), https://go.recordedfuture.com/hubfs/reports/ta-2023-0209.pdf.

68 Marcus Willet, "The Cyber Dimension of the Russia-Ukraine War," Survival 64, no. 5 (October 2022): 7–26.

69 Enhancing cybersecurity is a global imperative, with multilateral institutions such as the United Nations' International Telecommunications Union charting national government efforts to enact cybersecurity legislation, regulations to address privacy, unauthorized access, and online safety. International Telecommunication Union, *Global Cybersecurity Index 2020* (Geneva: International Telecommunications Union, 2021), https://www.itu.int/dms_pub/itu-d/opb/str/D-STR-GCI.01-2021-PDF-E.pdf

70 "Про рішення Ради національної безпеки і оборони України від 14 травня 2021 року 'Про Стратегію кібербезпеки України'" [On the decision of the National Security and Defense Council of Ukraine dated May 14, 2021 "On the Cybersecurity Strategy of Ukraine"], Legislation of Ukraine, August 26, 2021, https://zakon.rada.gov.ua/laws/show/447/2021#n7, Google Translate Ukrainian to English.

71 "Cybersecurity in Ukraine: National Strategy and international cooperation," The Global Forum on Cyber Expertise, July 6, 2017, https://thegfce.org/cybersecurity-in-ukraine-national-strategy-and-international-cooperation/; Ukraine's cybersecurity strategy has since been updated. See "Про рішення Ради національної безпеки і оборони України від 14 травня 2021 року 'Про Стратегію кібербезпеки України'" [The decision of the National Security and Defense Council of Ukraine dated May 14, 2021 "On the Cybersecurity Strategy of Ukraine,"], Legislation of Ukraine, August 26, 2021, https://zakon.rada.gov.ua/laws/show/447/2021#n7, Google Translate Ukrainian to English.

72 "Embassy Statement on the First US-Ukraine Bilateral Cyber Dialogue," U.S. Embassy in Ukraine, September 29, 2017, https://ua.usembassy.gov/embassy-statement-first-us-ukraine-bilateral-cyber-dialogue/.

73 Office of the Spokesperson, "U.S. Support for Connectivity and Cybersecurity in Ukraine - Fact Sheet," U.S. Department of State, May 10, 2022, https://www.state.gov/u-s-support-for-connectivity-and-cybersecurity-in-ukraine/

74 Foreign, Commonwealth and Development Office, "UK boosts Ukraine's cyber defences with £6 million support package," Press release, November 1, 2022, https://www.gov.uk/government/news/uk-boosts-ukraines-cyber-defences-with-6-million-support-package; and Office of the U.S. Spokesperson, "U.S. Support for Connectivity and Cybersecurity in Ukraine."

75 Office of the U.S. Spokesperson, "U.S. Support for Connectivity and Cybersecurity in Ukraine."

76 European Union External Action, "Ukraine and EU held the second round of the UA-EU Cybersecurity Dialogue," News release, September 29, 2022, https://www.eeas.europa.eu/eeas/ukraine-and-eu-held-second-round-ua-eu-cybersecurity-dialogue_en; and Laurens Cerulus, "EU to mobilize cyber team to help Ukraine fight Russian cyberattacks," *Politico*, February 21, 2022, https://www.politico.eu/article/ukraine-russia-eu-cyber-attack-security-help/amp/.

77 "Germany allocates extra 1 bln euros to Ukraine cyber-defence, documenting war crimes," Reuters, November 11, 2022, https://www.reuters.com/world/europe/germany-allocates-extra-1-bln-euros-ukraine-cyber-defence-documenting-war-crimes-2022-11-11/.

78 Alexander Martin, "Dutch intelligence: Many cyberattacks by Russia are not yet public knowledge," The Record, February 2022, 2023, https://therecord.media/dutch-intelligence-russia-cyberattacks-many-not-yet-public-knowledge.

79 "Ukraine cyber defenders in UK for high-level talks," National Cyber Security Centre, January 19, 2023, https://www.ncsc.gov.uk/news/ukraine-cyber-defenders-in-uk-for-high-level-talks.

80 The central role of the private sector has been recognized in a number of national cyber security strategies worldwide, and the United States has been particularly vocal about the importance of public-private partnerships in recent years. For the latest iteration, see The White House, "National Cybersecurity Strategy," Fact sheet, March 2, 2023, https://www.whitehouse.gov/briefing-room/statements-releases/2023/03/02/fact-sheet-biden-harris-administration-announces-national-cybersecurity-strategy/.

81 David E. Sanger, Julian E. Barnes, and Kate Conger, "As Tanks Rolled Into Ukraine, So Did Malware. Then Microsoft Entered the War," *New York Times,* February 28, 2022, https://www.nytimes.com/2022/02/28/us/politics/ukraine-russia-microsoft.html.

82 Brad Smith, "Digital technology and the war in Ukraine," Microsoft, February 28, 2022, https://blogs.microsoft.com/on-the-issues/2022/02/28/ukraine-russia-digital-war-cyberattacks/.

83 Greg Rattray et al., *The Cyber Defense Assistance Imperative - Lessons from Ukraine* (Washington, DC: The Aspen Institute, February 2023), https://www.aspeninstitute.org/publications/the-cyber-defense-assistance-imperative-lessons-from-ukraine/.

84 Amazon Staff, "How Amazon is assisting in Ukraine," Amazon, December 1, 2022, https://www.aboutamazon.com/news/community/amazons-assistance-in-ukraine; Phil Venables, "Google Cloud's security and resiliency measures for customers and partners," Google Cloud Blog, March 3, 2022, https://cloud.google.com/blog/products/identity-security/how-google-cloud-is-helping-those-affected-by-war-in-ukraine; and Brad Smith, "Defending Ukraine: Early Lessons from the Cyber War," Microsoft, June 22, 2022, https://blogs.microsoft.com/on-the-issues/2022/06/22/defending-ukraine-early-lessons-from-the-cyber-war/.

85 Matt Burgess, "Ukraine's Volunteer 'IT Army' is Hacking in Unchartered Territory," *Wired*, February 27, 2022, https://www.wired.co.uk/article/ukraine-it-army-russia-war-cyberattacks-ddos.

86 "Ministry of Digital Transformation: IT army blocks Russian sites in a few minutes - the main victories of Ukraine on the cyber front," Ukrainian Government, February 28, 2022, https://www.kmu.gov.ua/en/news/mincifri-it-armiya-blokuye-rosijski-sajti-za-dekilka-hvilin-golovni-peremogi-ukrayini-na-kiberfronti.

87 IT ARMY of Ukraine Telegram channel.

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

89 Dan Ciuriak, "Social Media Warfare Is Being Invented in Ukraine," Centre for International Governance Innovation, June 15, 2022, https://www.cigionline.org/articles/social-media-warfare-is-being-invented-in-ukraine/

90 Kyle Chayka, "Watching the World's 'First TikTok War'," March 3, 2022, *New Yorker*, https://www.newyorker.com/culture/infinite-scroll/watching-the-worlds-first-tiktok-war

91 Scott Nover, "TikTok suspends posting and live-streaming in Russia over 'fake news' law," Quartz, March 6, 2022, https://qz.com/2138322/tiktok-suspends-posting-and-live-streaming-in-russia https://www-spglobal-com.ezp-prod1.hul.harvard.edu/marketintelligence/en/news-insights/latest-news-headlines/big-tech-navigates-operating-social-pressures-amid-russia-ukraine-conflict-69208478.

92 Taylor Lorenz, "White House Press Briefing TikTokers Ukraine," SoundCloud, March 10, 2022, https://

soundcloud.com/taylorlorenz/white-house-press-briefing-tiktokers-ukraine.

93 Regarding the new norms of cyber warfare, see Commander Jacob Galbreath, Head of Strategy at NATO Cooperative Cyber Defence Centre of Excellence, quoted in Gerrard Cowan, "Russia-Ukraine: New Norms in Cyber Warfare Emerging," *Infosecurity Magazine*, February 23, 2023, https://www.infosecurity-magazine.com/news-features/new-norms-cyber-war/. Sweden established a Psychological Defence Agency in 2022, partly over concern of interference in its 2018 elections. See agency website, https://www.mpf.se/en/mission/.

94 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/.

95 Elon Musk (@elonmusk), "In addition to terminals, we have to create, launch, maintain & replenish satellites & ground stations & pay telcos for access to Internet via gateways. We've also had to defend against cyberattacks & jamming, which are getting harder. Burn is approaching ~$20M/month." Twitter post, October 14, 2022, 2:44 a.m., https://twitter.com/elonmusk/status/1580811694225653760.

96 "Safeguarding Ukraine's data to preserve its present and build its future," Amazon, June 9, 2022, https://www.aboutamazon.com/news/aws/safeguarding-ukraines-data-to-preserve-its-present-and-build-its-future.

97 "Secretary of Defense Lloyd J. Austin III and General Mark A. Milley Press Conference Following Ukraine Defense Contact Group Meeting, Ramstein Air Base, Germany," U.S. Department of Defense, January 20, 2023, https://www.defense.gov/News/Transcripts/Transcript/Article/3273771/secretary-of-defense-lloyd-j-austin-iii-and-general-mark-a-milley-press-confere/; and "UK's Sunak promises long-term support to Ukraine after drone attacks," Reuters, January 3, 2023, https://www.reuters.com/world/europe/uks-sunak-promises-long-term-support-ukraine-after-drone-attacks-2023-01-03/.

98 Alex Hern, "Elon Musk's SpaceX says it can no longer fund Starlink internet in Ukraine," *The Guardian*, October 14, 2022, https://www.theguardian.com/world/2022/oct/14/elon-musk-spacex-no-longer-fund-starlink-internet-ukraine.

99 Veronika Melkozerova, "Ukraine's Drone Academy is in session," *Politico*, February 26, 2023, https://www.politico.eu/article/ukraine-drone-academy-war-russia-kyiv-pilot/.

100 Jonathan Beale, "Ukraine-Russia: Hidden tech war as Slovyansk battle looms," BBC, July 8, 2022, https://www.bbc.co.uk/news/world-europe-62090791.

101 "DJI Reassesses Sales Compliance Efforts In Light Of Current Hostilities," DJI, April 26, 2022, https://www.dji.com/newsroom/news/dji-statement-on-sales-compliance-efforts#:~:text=DJI%20Reassesses%20Sales%20Compliance%20Efforts%20In%20Light%20Of%20Current%20Hostilities,-News-2022%2D04&text=DJI%20is%20internally%20reassessing%20compliance,activities%20in%20Russia%20and%20Ukraine.

102 Bart Hogeveen, *The UN norms of responsible state behaviour in cyberspace: Guidance on implementation for Member States of ASEAN* (Australian Strategic Policy Institute, March 2022), https://documents.unoda.org/wp-content/uploads/2022/03/The-UN-norms-of-responsible-state-behaviour-in-cyberspace.pdf.

103 "Responsible Cyber Power in Practice (HTML)," Gov.UK, April 4, 2023, https://www.gov.uk/government/publications/responsible-cyber-power-in-practice/responsible-cyber-power-in-practice-html.

104 Lisa Ferdinando, "Dempsey: Cyber Vulnerabilities Threaten National Security," DoD News, Defense Media Activity, Joint Chiefs of Staff, https://www.jcs.mil/Media/News/News-Display/Article/571809/dempsey-cyber-vulnerabilities-threaten-national-security/.

105 "UK and US call out Russia for SolarWinds compromise," National Cyber Security Centre, April 15, 2021, https://www.ncsc.gov.uk/news/uk-and-us-call-out-russia-for-solarwinds-compromise; "U.S. Government

Attributes Cyberattacks on SATCOM Networks to Russian State-Sponsored Malicious Cyber Actors," Cybersecurity and Infrastructure Security Agency, May 10, 2022, https://www.cisa.gov/news-events/alerts/2022/05/10/us-government-attributes-cyberattacks-satcom-networks-russian-state#:~:text=CISA%20and%20the%20Federal%20Bureau,state%2Dsponsored%20malicious%20cyber%20actors; and Antony Blinken, "Attribution of Russia's Malicious Cyber Activity Against Ukraine," U.S. Department of State, May 10, 2022, https://www.state.gov/attribution-of-russias-malicious-cyber-activity-against-ukraine/.

106 "FAQ: Direct Participation in Hostilities: Questions & Answers," International Committee of the Red Cross, June 2, 2009, https://www.icrc.org/en/doc/resources/documents/faq/direct-participation-ihl-faq-020609.htm#:~:text=Persons%20participate%20directly%20in%20hostilities,enemy's%20military%20operations%20or%20capacity.

107 Jason Healey and Olivia Grinberg, "Patriotic Hacking is No Exception," Lawfare, September 27, 2022, https://www.lawfareblog.com/patriotic-hacking-no-exception; and Peter Pascucci and Kurt Sanger, "Cyber Norms in the Context of Armed Conflict," Lawfare, November 16, 2022, https://www.lawfareblog.com/cyber-norms-context-armed-conflict.

108 Dan Milmo, "Amateur hackers warned against joining Ukraine's 'IT army'," *The Guardian*, March 18, 2022, https://www.theguardian.com/world/2022/mar/18/amateur-hackers-warned-against-joining-ukraines-it-army; and Pascucci and Sanger, "Cyber Norms in the Context of Armed Conflict."

109 State Service of Special Communications and Information Protection of Ukraine, *War in Ukraine: Pulse of. Cyber Defense* (State Service of Special Communications and Information Protection of Ukraine, February 2023). https://techukraine.org/2023/01/09/war-in-ukraine-pulse-of-cyber-defense-september-december-2022/.

110 Jeremy Fleming, "The head of GCHQ says that Vladimir Putin is losing the information war in Ukraine," *The Economist*, August 18, 2022, https://www.economist.com/by-invitation/2022/08/18/the-head-of-gchq-says-vladimir-putin-is-losing-the-information-war-in-ukraine.

111 In September 2022, the Tony Blair Institute for Global Change held a closed roundtable in Washington D.C. with public policy representatives from platforms, content distribution networks, former government representatives, think tanks, and civil society organisations to set out recommendations for private actor involvement in geopolitical crises. The meeting was held under the Chatham House rule and ideas expressed in this paper are drawn from the shared themes.

112 Wilde, *Cyber Operations in Ukraine*.

113 Ibid.

114 Pete Furlong, Melanie Garson, and Jeegar Kakkad, "Software and Hard War: Building Intelligent Power for Artificially Intelligent Warfare," Tony Blaire Institute for Global Change, November 18, 2022, https://www.institute.global/insights/geopolitics-and-security/software-and-hard-war-building-intelligent-power-artificially-intelligent-warfare.

115 John McDowell, "Enormous (Mega) Satellite Constellations," Jonathan Space Pages, https://planet4589.org/space/con/conlist.html.

116 "Google + Mandiant Transforming Security Operations and Incident Response," Google Cloud, September 12, 2022, https://cloud.google.com/blog/products/identity-security/google-completes-acquisition-of-mandiant.

117 Smith, "Defending Ukraine: Early Lessons from the Cyber War."

118 João Tomé, David Belson, and Kristin Berdan, "One year of war in Ukraine: Internet trends, attacks, and resilience," Cloudflare Blog, February 23, 2023, https://blog.cloudflare.com/one-year-of-war-in-ukraine/.

119 Kevin Limonier et al., "Mapping the routes of the Internet for geopolitics: the case of Eastern Ukraine," *First Monday* 26, no. 5 (2021).

120 State Service of Special Communications and Information Protection of Ukraine, "Yurii Schchyhol: the Russian Federation has turned even communication into a weapon," Press release, September 27, 2022, https://cip.gov.ua/en/news/yurii-shigol-rosiiska-federaciya-peretvorila-na-zbroyu-navit-zv-yazok.

121 State Service of Special Communications and Information Protection of Ukraine, "Invaders use blackmailing and intimidation to force Ukrainian Internet service providers to connect to Russian networks," Press release, May 13, 2022, https://cip.gov.ua/en/news/okupanti-shantazhem-i-pogrozami-zmushuyut-ukrayinskikh-provaideriv-pidklyuchatisya-do-rosiiskikh-merezh.

122 C. Miller, M. Scott, and B. Bender, "UkraineX: How Elon Musk's space satellites changed the war on the ground," *Politico*, June 8, 2022, https://www.politico.eu/article/elon-musk-ukraine-starlink/.

123 Tomé, Belson, and Berdan, "One year of war in Ukraine."

124 Rishi Iyengar, "This is different: Why internet backbone services are cutting off Russia," CNN, March 14, 2022, https://edition.cnn.com/2022/03/11/tech/russia-internet-backbone-cogent-lumen/index.html.

125 "Threats," CyberPeace Institute, https://cyberconflicts.cyberpeaceinstitute.org/threats.

126 Tomé, Belson, and Berdan, "One year of war in Ukraine."

127 Microsoft, *Digital Defense Report 2022* (Redmond, WA: Microsoft, 2022), https://query.prod.cms.rt.microsoft.com/cms/api/am/binary/RE5bUvv?culture=en-us&country=us.; and Microsoft, *Defending Ukraine: Early Lessons from the Cyber War.*

128 Matt Olney, "Cisco stands on guard with our customers in Ukraine," Cisco Talos, March 3, 2022.

129 Huntley, "Fog of war."

130 "Defending Ukraine: Early Lessons from the Cyber War," Microsoft.

131 Mike Moore, "Ukraine hails 'priceless' help from Amazon Web Services," techradar.pro, December 6, 2022.

132 Oliver Tavakoli, "Russian Wiper Malware is Novel – Protecting Against it Need Not Be," Vectra, February 25, 2022, https://www.vectra.ai/blogpost/russian-wiper-malware-is-novel-protecting-against-it-need-not-be; and Michael Hill, "How security vendors are aiding Ukraine," CSO, March 2, 2022, https://www.csoonline.com/article/3651685/how-security-vendors-are-aiding-ukraine.html.

133 For example, Fastly, which has only a 5 percent market share, had an outage in June 2021 which in turn affected access to Amazon, Reddit, Hulu, CNN, Vimeo, and UK government sites.

134 Matthew Prince, "Cloudflare's services in Ukraine, Belarus and Russia," Cloudflare, March 7, 2022, https://blog.cloudflare.com/steps-taken-around-cloudflares-services-in-ukraine-belarus-and-russia/.

135 Ayesha Rascoe, "Some Russians are skirting website restrictions through VPNs. What are they?," WFDD, April 3, 2022, https://www.wfdd.org/story/some-russians-are-skirting-website-restrictions-through-vpns-what-are-they.

136 Alex Horton and Shane Harris, "Russian troops' tendency to talk on unsecured lines is proving costly," *Washington Post,* March 27, 2022, https://www.washingtonpost.com/national-security/2022/03/27/russian-military-unsecured-communications/.

137 Patrick Tucker, "What Surprised One Drone Maker About Russia's War on Ukraine," Defense One, October

3, 2022, https://www.defenseone.com/technology/2022/10/what-surprised-one-drone-maker-about-russias-war-ukraine/377994/.

138 "YouTube Blocked in Ukraine's Russian-Occupied Kherson," *Moscow Times*, July 6, 2022, https://www.themoscowtimes.com/2022/07/06/youtube-blocked-in-russia-occupied-kherson-a78220.

139 "#KeepItOn: Who is shutting down the internet in Ukraine?" AccessNow, March 17, 2023, https://www.accessnow.org/who-is-shutting-down-the-internet-in-ukraine/.

140 James Vincent, "Google disables Maps traffic data in Ukraine to protect citizens," The Verge, February 28, 2022, https://www.theverge.com/2022/2/28/22954426/google-disables-maps-traffic-data-in-ukraine-to-protect-citizens.

141 Shen Lu, "How China's social media handles fake news about Ukraine," Protocol, March 1, 2022, https://www.protocol.com/china/china-ukraine-war-misinformation.

142 Huntley, "Fog of war."

143 Microsoft, *Defending Ukraine: Early Lessons from the Cyber War.*

144 Daryna Antoniuk, "Ukraine reconsiders bug bounties after latest cyberattacks. But are they enough?" The Record, February 3, 2022, https://therecord.media/ukraine-reconsiders-bug-bounties-after-latest-cyberattacks-but-are-they-enough.

145 IT ARMY of Ukraine Telegram channel.

146 Alex Haynes, "Crowdsourced Security is out of Control in the Ukraine Conflict," United States Cybersecurity Magazine, https://www.uscybersecurity.net/crowdsourced-security-out-of-control-in-the-ukraine-conflict/.

147 Adam Bannister, "Concerns raised over bug disclosure program aimed at tackling Russia's 'propaganda machine," The Daily Swig, March 9, 2022, https://portswigger.net/daily-swig/concerns-raised-over-bug-disclosure-program-aimed-at-tackling-russias-propaganda-machine.

148 "U.S. moves to keep Russian people connected despite sanctions," AccessNow, April 8, 2022, https://www.accessnow.org/press-release/u-s-treasury-russia-sanctions-internet/.

149 Jagmeet Singh, "Ukraine Ethical Hackers Bewildered as HackerOne Bug Bounty Platform Said to Halt Their Payouts," Gadgets360, March 17, 2022, https://www.gadgets360.com/internet/news/ethical-hackers-ukraine-security-researchers-hackerone-bug-bounty-payouts-withhold-update-russia-2822078.

150 Mulsif Vengattil and Elizabeth Culliford, "Facebook allows war posts urging violence against Russian invaders," Reuters, March 11, 2022, https://www.reuters.com/world/europe/exclusive-facebook-instagram-temporarily-allow-calls-violence-against-russians-2022-03-10/.

151 Emerson T. Brooking, "Meta Meets the Reality of War," Slate, March 17, 2022, https://slate.com/technology/2022/03/meta-facebook-calls-violence-invading-russians.html.

152 Isabelle Khushudyan et al., "Musk threatens to stop funding Starlink internet Ukraine relies on in war," *Washington Post*, October 14, 2022, https://www.washingtonpost.com/world/2022/10/14/ukraine-elon-musk-starlink-ambassador-andrij-melnyk/.

153 Amritha Jayanti, "Starlink and the Russia-Ukraine War: A Case of Commercial Technology and Public Purpose?" Belfer Center for Science and International Affairs, March 9, 2022, https://www.belfercenter.org/publication/starlink-and-russia-ukraine-war-case-commercial-technology-and-public-purpose.

154 Jon Brodkin,"SpaceX says it blocked Ukriane from using Starlink with military drones," Ars Technica,

February 10, 2023, https://arstechnica.com/tech-policy/2023/02/spacex-says-it-blocked-ukraine-from-using-starlink-with-military-drones/.

155 "Is there a path ahead for peace in Ukraine?" Gzero Media, February 17, 2023, https://www.gzeromedia.com/global-stage/crisis-recovery/is-there-a-path-ahead-for-peace-in-ukraine.

156 "Remarks by President Biden and President Zelenskyy in Joint Statement," The White House, February 20, 2022, https://www.whitehouse.gov/briefing-room/speeches-remarks/2023/02/20/remarks-by-president-biden-and-president-zelenskyy-of-ukraine-in-joint-statement/.

157 Furlong, Garson, and Kakkad, "Software and Hard War."

158 Kim Zetter, "Security Firms Aiding Ukraine During War Could be Considered Participants in Conflict," Zero Day, December 7, 2022, https://zetter.substack.com/p/security-firms-aiding-ukraine-during.

159 Shaun Waterman, "Ukraine Scrambles to Draft Cyber Law, Legalizing Its Volunteer Hacker Army," *Newsweek,* March 14, 2023, https://www.newsweek.com/ukraine-drafting-new-law-legalizing-volunteer-hacker-cyber-army-red-cross-1786814.

160 Zetter, "Security Firms Aiding Ukraine During War Could be Considered Participants in Conflict."

161 North Atlantic Treaty Organization, "Prague Summit Declaration Issued by NATO Heads of State and Government (2021)," Press release, November 2, 2002, https://www.nato.int/cps/en/natohq/official_texts_19552.htm.

162 Neil Robinson and Chelsey Slack, "Co-operation: a key to NATO's cyberspace endeavour," *European Foreign Affairs Review* 24, no. 2 (2019).

163 See "Global Cyber Strategies Index," Center for Strategic and International Studies, https://www.csis.org/programs/strategic-technologies-program/archives/cybersecurity-and-governance/global-cyber; and Damjan Štrucl, *Comparative study on the cyber defence of NATO Member States* (Tallinn, Estonia: NATO CCD COE Publications, 2022).

164 "NATO 2022 Strategic Concept," North Atlantic Treaty Organization, https://www.nato.int/strategic-concept/; and Lydia Harriss and Amber Keegan, "States' use of cyber operations," UK Parliament, October 27, 2022, https://post.parliament.uk/research-briefings/post-pn-0684/.

165 This article will use the term "state-sponsored actors" to refer to malicious cyber activity that is carried out, directly or through state-sponsored cyber threat proxy groups, at the order of national governments.

166 Huntley, "Fog of war."

167 Ibid; Ilona Khmelova, *Cyber, Artillery, Propaganda: Comprehensive Analysis of Russian Warfare Dimensions* (Kyiv: Economic Security Council of Ukraine, 2022), https://nsarchive.gwu.edu/sites/default/files/documents/rr9q9n-glu5j/2023-01-17-Ukraine-ESCU-Cyber-Artiller-Propaganda-Comprehensive-Analysis-of-Russian-Warfare-Dimensions-ESCU.pdf.

168 Huntley, "Fog of war."

169 Microsoft Digital Security Unit, *An overview of Russia's cyberattack activity in Ukraine* (Redmond, WA: Microsoft, April 27, 2022), https://query.prod.cms.rt.microsoft.com/cms/api/am/binary/RE4Vwwd.

170 Harriss and Keenan, "States' use of cyber operations"; UK House of Commons Defence Committee, *Rash or Rational? North Korea and the Threat it Poses* (London: House of Commons, March 27, 2018, https://publications.parliament.uk/pa/cm201719/cmselect/cmdfence/327/327.pdf.

171 Huntley, "Fog of war."

172 "NATO reaffirms support for Albania following cyber attacks," North Atlantic Treaty Organization, September 22, 2022, https://www.nato.int/cps/en/natohq/news_207552.htm; "Significant Cyber Incidents," Center for Strategic and International Studies, https://www.csis.org/programs/strategic-technologies-program/significant-cyber-incidents; and "Iranian State Actors Conduct Cyber Operations Against the Government of Albania," Cybersecurity and Infrastructure Security Agency and Federal Bureau of Investigation Joint Cybersecurity Adversary, September 23, 2023, https://www.cisa.gov/news-events/cybersecurity-advisories/aa22-264a.

173 North Atlantic Treaty Organization, "NATO team in North Macedonia to help against hybrid attacks," News release, March 7, 2023, https://www.nato.int/cps/en/natohq/news_212621.htm?selectedLocale=en.

174 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/.

175 Huntley: "Fog of war."; Crowdstrike, *2023 Global Threat Report* (Austin, TX: Crowdstrike, 2023); Microsoft Threat Intelligence, *A Year of Russian Hybrid Warfare in Ukraine* (Redmond, WA: Microsoft, March 15, 2023), https://www.microsoft.com/en-us/security/business/security-insider/wp-content/uploads/2023/03/A-year-of-Russian-hybrid-warfare-in-Ukraine_MS-Threat-Intelligence-1.pdf; and Thales, *2022-2023: A Year of Cyber Conflict in Ukraine* (Paris: Thales, March 2023), https://bo-cyberthreat.thalesgroup.com/sites/default/files/2023-03/Brochure-resume-A5-WEB.pdf. See also "China Cyber Threat Overview and Advisories," Cybersecurity and Infrastructure Agency, https://www.cisa.gov/china.

176 Huntley, "Fog of war."

177 Lucas Kello, *The Virtual Weapon and International Order* (New Haven, CT: Yale University Press, 2017).

178 "NATO 2022 Strategic Concept," North Atlantic Treaty Organization; and Samuel Zilincik and Isabelle Duyvesteyn. "Strategic studies and cyber warfare." *Journal of Strategic Studies* (2023): 1-22.

179 "Significant Cyber Incidents," Center for Strategic and International Studies.

180 Khmelova, *Cyber, Artillery, Propaganda*.

181 "NATO 2022 Strategic Concept," North Atlantic Treaty Organization, paragraph 8.

182 Ibid., paragraph 13.

183 Tobias Bunde et al., *Re:vision: Munich Security Report* 2023Munich (Munich: Munich Security Conference, 2023), https://securityconference.org/en/publications/munich-security-report-2023/.

184 The White House, *National Cybersecurity Strategy 2023* (Washington, DC: The White House, March 2023), https://www.whitehouse.gov/wp-content/uploads/2023/03/National-Cybersecurity-Strategy-2023.pdf.

185 "NATO 2022 Strategic Concept," paragraph 25, North Atlantic Treaty Organization; and North Atlantic Treaty Organization, "Brussels Summit Communiqué," Press release, June 14, 2021, paragraph 32, https://www.nato.int/cps/en/natohq/news_185000.htm?selectedLocale=en.

186 See, for example, Tim Stevens, "A cyberwar of ideas? Deterrence and norms in cyberspace," *Contemporary Security Policy* 33, no. 1 (2012): 148-70; Mariarosaria Taddeo, "The limits of deterrence theory in cyberspace," *Philosophy & Technology* 31, no. 3 (2018): 339-55; and Stefan Soesanto and Max Smeets, "Cyber deterrence: the past, present, and future," *NL ARMS Netherlands Annual Review of Military Studies 2020: Deterrence in the 21st Century—Insights from Theory and Practice* (2021): 385-400.

187 For academic discussions on this topic, see Martin C. Libicki, "Expectations of Cyber Deterrence," *Strategic Studies Quarterly* 12, no. 4 (2018): 44-57, https://www.jstor.org/stable/26533614; Nori Katagiri, "Three Conditions for Cyber Countermeasures: Opportunities and Challenges of Active-Defense

Operations," The Cyber Defense Review 7, no. 3 (2022): 79–90, https://www.jstor.org/stable/48682324.

188 Nori Katagiri, "Why international law and norms do little in preventing non-state cyber attacks," *Journal of Cybersecurity* 7, no. 1 (2021).

189 North Atlantic Treaty Organization, "Brussels Summit Declaration," Press release, July 11, 2018, https://www.nato.int/cps/en/natohq/official_texts_156624.htm; and NATO, "Statement by NATO Heads of State and Government," Press release, March 24, 2022, https://www.nato.int/cps/en/natohq/official_texts_193719.htm.

190 North Atlantic Treaty Organization, "Madrid Summit Declaration," Press release, June 29, 2022, https://www.nato.int/cps/en/natohq/official_texts_196951.htm?selectedLocale=en.

191 "Resilience, Civil Preparedness and Article 3," North Atlantic Treaty Organization, updated September 20, 2022, https://www.nato.int/cps/en/natohq/topics_132722.htm. While NATO does not have a formal definition for cyber resilience, NIST defines the term as "the ability to anticipate, withstand, recover from, and adapt to adverse conditions, stresses, attacks, or compromises on systems that use or are enabled by cyber resources." "Glossary: Cyber Resilience (Source: NIST SP 800-172)," NIST Computer Security Resource Center, National Institute for Standards and Technology, https://csrc.nist.gov/glossary/term/cyber_resiliency. For a discussion on NATO's approach to the principles of cyber resilience, see Alexander Kott et al., "Approaches to enhancing cyber resilience: report of the North Atlantic Treaty Organization (NATO) workshop IST-153," arXiv:1804.07651 (2018), https://arxiv.org/abs/1804.07651; Jamie Shea, "Resilience: a core element of collective defence," *NATO Review* 30, no. 03 (2016); and NATO summit statements, including the 2021 Brussels Communiqué and the 2022 Madrid Summit Declaration.

192 The White House, *National Cybersecurity Strategy*; "Directive on Measures for a High Common Level of Cybersecurity across the Union (NIS2 Directive)," European Commission, https://digital-strategy.ec.europa.eu/en/policies/nis2-directive; European Council, "EU Resilience: Council Adopts a Directive to Strengthen the Resilience of Critical Entities," Press release, https://www.consilium.europa.eu/en/press/press-releases/2022/12/08/eu-resilience-council-adopts-a-directive-to-strengthen-the-resilience-of-critical-entities/.

193 See EUCyberDirect's Cyber Diplomacy Atlas for an analysis of national approaches to cyber defence, available at https://eucyberdirect.eu/atlas. See also Alessandro Marrone and Ester Sabatino, *Cyber Defence in NATO Countries: Comparing Models* (Rome: IAI, 2021), https://www.iai.it/en/pubblicazioni/cyber-defence-nato-countries-comparing-models.

194 "The North Atlantic Treaty," North Atlantic Treaty Organization, https://www.nato.int/cps/en/natolive/official_texts_17120.htm.

195 "Cyber Defence," North Atlantic Treaty Organization, https://www.nato.int/cps/en/natohq/topics_78170.htm; "Resilience, Civil Preparedness and Article 3," North Atlantic Treaty Organization; and Wolf-Diether Roepke and Hasit Thankey, "Resilience: the first line of defence," NATO Review 27, no. 02 (2019).

196 Max Smeets, *No Shortcuts: Why states struggle to develop a military cyber-force* (Oxford: Oxford University Press, 2022).

197 James Lewis, "Cyber War and Ukraine," Center for Strategic and International Studies, *White Paper*, June 16, 2022, https://www.csis.org/analysis/cyber-war-and-ukraine; Wilde, *Cyber Operations in Ukraine*; Sean Atkins, "A web of partnerships: Ukraine, operational collaboration, and effective national defense in cyberspace," Atlantic Council, August 30, 2022, https://www.atlanticcouncil.org/content-series/airpower-after-ukraine/a-web-of-partnerships-ukraine-operational-collaboration-and-effective-national-defense-in-cyberspace/; and Office of the U.S. Spokesperson, "U.S. Support for Connectivity and Cybersecurity in Ukraine."

198 Lewis, "Cyber War and Ukraine"; and 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.

199 The White House, *National Cybersecurity Strategy*; and North Atlantic Treaty Organization, "Madrid Summit Declaration," Press release, paragraph 10.

200 Amy Ertan et al., *Cyber Exercises: A Vision for NATO CyCon 2021 Workshop Summary Report* (Tallinn, Estonia: NATO CCD COE Publications, August 2021), https://ccdcoe.org/uploads/2022/07/Cyber-Exercises-A-Vision-for-NATO-Summary-Doc-August-2021.pdf.

201 Dan Black, *Russia's War in Ukraine: Examining the Success of Ukrainian Cyber Defences* (London: International Institute for Strategic Studies, March 2023); European Union External Action Service, "Ukraine and EU held the second round of the UA-EU Cybersecurity Dialogue," Press release, September 2022, https://www.eeas.europa.eu/eeas/ukraine-and-eu-held-second-round-ua-eu-cybersecurity-dialogue_en; and Beecroft, "Evaluating the International Support to Ukrainian Cyber Defense."

202 See, for instance, "Russia Ukraine Crisis Overview," Accenture, June 10, 2022, https://www.accenture.com/us-en/blogs/cyber-defense/ukraine-russia-2022.

203 "Safeguarding Ukraine's data to preserve its present and build its future," Amazon; and Bateman, *Russia's Wartime Cyber Operations in Ukraine*.

204 See, for instance, "Russia Ukraine Crisis Overview," Accenture, June 10, 2022, https://www.accenture.com/us-en/blogs/cyber-defense/ukraine-russia-2022; "Safeguarding Ukraine's data to preserve its present and build its future," Amazon; Bateman, *Russia's Wartime Cyber Operations in Ukraine;* Jurgita Lapienytė, "Google offers free DDoS protection to Ukrainian organizations," Cybernews, March 13, 2022, https://cybernews.com/news/google-offers-free-ddos-protection-to-ukrainian-organizations/; and Stephanie Pell, "Private-Sector Cyber Defense in Armed Conflict," Lawfare, December 1, 2022, https://www.lawfareblog.com/private-sector-cyber-defense-armed-conflict.

205 Emma Schroeder and Sean Back, *A Parallel Terrain: Public-Private Defense of the Ukrainian Information Environment* (Washington, DC: Atlantic Council, Cyber Statecraft Initiative and DFRLab, February 27, 2023), https://www.atlanticcouncil.org/in-depth-research-reports/report/a-parallel-terrain-public-private-defense-of-the-ukrainian-information-environment/#executivesummary; and Pell, "Private-Sector Cyber Defense in Armed Conflict."

206 Ibid.

207 Прес-офіс Міністерства [Press Office of the Ministry], "Михайло Федоров вручив першу «Відзнаку миру» компанії Google" [Mykhailo Fedorov presented the first 'Peace prize' to Google], May 25, 2022, Ministry of Digital Transformation, https://thedigital.gov.ua/news/mikhaylo-fedorov-vruchiv-pershu-vidznaku-miru-kompanii-google. English translation is shown below Ukrainian text.

208 Ines Kagubare, "Russia-Ukraine war has improved US cyber cooperation, says key official," *The Hill*, February 2, 2023, https://thehill.com/policy/cybersecurity/3841444-russia-ukraine-war-has-improved-us-cyber-cooperation-says-key-official/.

209 Kari A. Bingin, Kaitlyn Johnson, and Zhanna Malekos Smith, "Russia Threatens to Target Commercial Satellites," CSIS, *Critical Questions*, November 10, 2022, https://www.csis.org/analysis/russia-threatens-target-commercial-satellites; and Ellen Nakashima, "Russian military behind hack of satellite communication devices in Ukraine at war's outset, U.S. officials say," *Washington Post*, March 24, 2022, https://www.washingtonpost.com/national-security/2022/03/24/russian-military-behind-hack-satellite-communication-devices-ukraine-wars-outset-us-officials-say/.

210 Schroeder and Back, *A Parallel Terrain*.

211 Jack Detsch and Robbie Gramer, "Starlink Cuts Off Ukrainian Drones," *Foreign Policy*, February 9, 2023, https://foreignpolicy.com/2023/02/09/ukraine-russia-war-starlink-drones-musk-spacex/.

212 "Musk says SpaceX cannot fund Ukraine's Starlink 'indefinitely'," Al Jazeera, October 14, 2022, https://www.aljazeera.com/news/2022/10/14/musk-says-spacex-cannot-fund-ukraines-internet.

213 Tara Subramaniam et al., "January 26, 2023 - Russia-Ukraine news," CNN, January 26, 2023, https://edition.cnn.com/europe/live-news/russia-ukraine-war-news-1-26-23/h_a9d1cbe459b1c0caeb9b638a418bd645; and "Poland transfers 8,000 Starlink terminals to Ukraine," *Militarnyi*, January 14, 2023, https://mil.in.ua/en/news/poland-transfers-8-000-starlink-terminals-to-ukraine/.

214 Gareth Corfield, "Microsoft Declines New Cloud Customers after Promise to Ukraine," *The Telegraph*, July 2, 2022, https://www.telegraph.co.uk/business/2022/07/02/microsoft-declines-new-cloud-customers-promise-ukraine/.

215 Schroeder and Back, *A Parallel Terrain*.

216 Ibid; and Smith, "Extending our vital technology support for Ukraine."

217 Louise Marie Hurel and Luisa Cruz Lobato, "Unpacking cyber norms: private companies as norm entrepreneurs," *Journal of Cyber Policy* 3, no. 1 (2018): 61–76.

218 Nicholas Camus, "Elon Musk says SpaceX restricted internet in Ukraine to prevent escalation 'that may lead to WW3'," *Politico*, February 13, 2023, https://www.politico.eu/article/spacex-restricted-internet-ukraine-prevent-escalation-elon-musk-russia-starlink-ww3-gwynne-shotwell-drones-infrastructure/; https://mil.in.ua/en/news/spacex-curbed-ukraine-s-use-of-starlink-terminals/.

COVER PHOTO
SYDA PRODUCTIONS VIA ADOBE STOCK

CSIS | CENTER FOR STRATEGIC & INTERNATIONAL STUDIES

1616 Rhode Island Avenue NW
Washington, DC 20036
202 887 0200 | **www.csis.org**