Texas National Security Review: Volume 5, Issue 3 (Summer 2022)
Print: ISSN 2576-1021 Online: ISSN 2576-1153

Why Cyber Dogs Have Yet to Bark Loudly in Russia's Invasion of Ukraine

Nadiya Kostyuk
Erik Gartzke

Prior to the Russian invasion of Ukraine, pundits agreed that the ongoing crisis was likely to involve extensive cyber conflict. Some argued that cyber war would accompany traditional forms of warfare. Others claimed that cyber conflict would substitute for a physical conflict. However, the modest scale of Russia's cyber attacks has fallen far short of these predictions. We explain this surprising situation by arguing that, while not directly causally related, cyber and conventional conflict are indirectly intertwined, through evolving macro-economic trends. The same factors that encourage modern states to integrate economically also increasingly cause them to compete over information rather than over territory.

As Russia's massive armored buildup on the Ukrainian border became apparent in the fall of 2021, pundits began to offer contrasting predictions about the likely role that cyber war would play in any escalation of the crisis.[1] These disparate claims mirror a larger ongoing debate about whether cyber war is more likely to supplant or exacerbate traditional modes of warfare in the 21st century. Specifically, advocates of the theory that cyber operations will increasingly substitute for conventional conflict argue that cyber conflict today and in the future could achieve what tanks did in the 20th century.[2] Advocates of a competing theory argue that cyber operations will tend to coincide with, rather than replace, any significant use of military force.

While Russia has conducted some cyber operations in Ukraine, both in the lead-up to and after the February invasion, these have neither supplanted nor significantly supplemented conventional combat activities. Given Russia's highly sophisticated cyber capabilities and its long-term presence in Ukrainian networks,[3] why has it failed to utilize such apparently potent tools in seeking strategic or tactical advantages?

The answer to this perplexing question can be gleaned from a more systematic empirical assessment of cyber conflict. In a recent study, we examined whether cyber operations mostly serve as complements to, or substitutes for, conventional conflict, or whether the two forms of conflict more often occur independently.[4] Our statistical analysis of global conventional military campaigns over an 11-year period suggests that, with a few notable exceptions, cyber operations are rarely used as either complements to or substitutes for conventional military operations. Instead, countries tend most often to use these two types of operations independently of one another, due to both the difficulty of coordinating them and the different political purposes served by the two modes of conflict. Ultimately, our results show that, while cyber operations are far more likely to be used independently of conventional warfare than as a direct substitute for or complement to it, there is an *indirect* link between cyber and conventional conflict: The more

[1] Keir Giles, "Putin Does Not Need to Invade Ukraine to Get His Way," Chatham House, Dec. 21, 2021, https://www.chathamhouse.org/2021/12/putin-does-not-need-invade-ukraine-get-his-way; Martin Matishak, "Russia Could Launch Digital Offensive Against Ukraine, Administration Official Warns," *The Record*, Dec. 6, 2021, https://therecord.media/russia-could-launch-digital-offensive-against-ukraine-administration-official-warns; Jason Healey, "Preparing for Inevitable Cyber Surprise," *War on the Rocks*, Jan. 12, 2022, https://warontherocks.com/2022/01/preparing-for-inevitable-cyber-surprise/; and William Courtney and Peter A. Wilson, "If Russia Invaded Ukraine," RAND Corp., Dec. 8, 2021, https://www.rand.org/blog/2021/12/expect-shock-and-awe-if-russia-invades-ukraine.html.

[2] Richard A. Clarke and Robert K. Knake, *Cyber War: The Next Threat to National Security and What to Do About It* (New York: Ecco, 2010); Nuno P. Monteiro and Alexandre Debs, "The Strategic Logic of Nuclear Proliferation," *International Security* 39, no. 2 (Fall 2014): 7–51), https://www.jstor.org/stable/24480582; Lucas Kello, "The Meaning of the Cyber Revolution: Perils to Theory and Statecraft," *International Security* 38, no. 2 (Fall 2013): 7–40; and Billy K. Rios, *Sun Tzu Was a Hacker: An Examination of the Tactics and Operations from a Real World Cyber Attack*," The Virtual Battlefield: Perspectives on Cyber Warfare 3, no. 143, (2009), https://ccdcoe.org/uploads/2018/10/10_RIOS_Sun_Tzu_was_a_hacker.pdf.

[3] Mark Pomerleau, "Russia and China Devote More Cyber Forces to Offensive Operations than US, Says New Report," *C4ISRNet*, Feb. 14, 2022, https://www.c4isrnet.com/cyber/2022/02/14/russia-and-china-devote-more-cyber-forces-to-offensive-operations-than-us-says-new-report/#.

[4] Nadiya Kostyuk and Erik Gartzke, "Fighting in Cyberspace: Internet Dependency and the Substitutability of Cyber and Military Operations," Presented at the 2019 International Studies Association Conference. For the latest version of manuscript (Jan. 18, 2022), see https://www.dropbox.com/s/x4xxw0wgb1jgx7f/CCO_GK_112121.pdf?dl=0.

access a country has to the internet, the more likely it will be involved in cyber conflict, whether as the target or the aggressor. We call this effect "indirect substitution."

In this article, we apply our more general argument to explain Russia's limited cyber efforts in Ukraine. We start by discussing the most prevalent theories regarding a direct relationship between cyber and military operations, including a summary of our own research. We then go on to explain the theory of indirect substitution. Next, we apply these theories to explain Russia's cyber efforts in Ukraine. Then, we refute a number of alternative explanations for Russia's limited visible cyber efforts in Ukraine. Finally, we conclude with some lessons for future conflicts.

Existing and Proposed Theories of the Relationship Between Cyber and Conventional Conflict

Direct Links Between Cyber and Military Operations

Existing theories of cyber conflict posit one of several possible direct links between cyber and conventional modes of combat. Most commonly, cyber conflict is viewed as either a direct substitute for or a complement to conventional conflict.[5]

Cyber Conflict as a Substitute

Advocates of the substitution theory argue that states should be able to use cyber operations to degrade or destroy enemy capabilities in peacetime, rather than being forced to initiate and engage in costly conflicts in the physical world.[6] By doing so, leaders can deny responsibility for damaging and invasive operations, lowering the prospect of incurring harmful retaliation from the target and limiting blowback at home.[7]

There are, indeed, cyber operations aimed at disruption and degradation that can serve as strategic substitutes for military operations. For instance, the Stuxnet worm — an allegedly joint operation between the United States and Israel — targeted an Iranian nuclear enrichment facility to slow down the country's development of a nuclear weapon.[8] These governments strategically used Stuxnet as a substitute for a more escalatory military option: Israeli air strikes.[9] As an alternative to full-scale war, the U.S. government also developed a comprehensive cyber-attack plan called *Nitro Zeus* to disrupt and degrade vital systems of Iran's infrastructure.[10]

Cyber Conflict as a Complement

On the other hand, advocates of the complementarity theory argue that governments can use cyber operations during combat to affect the balance of military power.[11] In other words, they claim that cyber operations can exploit a target's unrecognized vulnerabilities, allowing attackers to disrupt an opponent's command and control, hindering communication and creating obstacles to the opponent's ability to sustain military operations.

Disruption and degradation operations might be useful complementary tools of combat because they focus on degrading an enemy's command and con-

[5] Monteiro and Debs, "The Strategic Logic of Nuclear Proliferation"; T.V. Paul, "Disarmament Revisited: Is Nuclear Abolition Possible?" *Journal of Strategic Studies* 35, no. 1 (2012): 149–69, https://doi.org/10.1080/01402390.2012.645369; Bryan Robert Early and Christopher Way, "First Missiles, then Nukes? Explaining the Connection Between Missile Programs and the Proliferation of Nuclear Weapons," *Korean Journal of International Studies* 15, no. 3 (December 2017): 359–89, https://dx.doi.org/10.14731/kjis.2017.12.15.3.359; and Michael C. Horowitz and Neil Narang, "Poor Man's Atomic Bomb? Exploring the Relationship Between 'Weapons of Mass Destruction,'" *Journal of Conflict Resolution* 58, no. 3 (April 2014): 509–35, https://www.jstor.org/stable/24545650.

[6] Clarke and Knake, *Cyber War*; David S. Fadok, "Book Review: Cyber War: The Next Threat to National Security and What to Do About It," *Strategic Studies Quarterly* 5, no. 4 (Winter 2011): 133–35, https://www.jstor.org/stable/26270542; Kello, "The Meaning of the Cyber Revolution"; and Rios, "Sun Tzu was a Hacker."

[7] Erica D. Borghard and Shawn W. Lonergan, "The Logic of Coercion in Cyberspace," *Security Studies* 26, no. 3 (2017): 452–81, https://doi.org/10.1080/09636412.2017.1306396; and Brandon Valeriano, Benjamin Jensen, and Ryan C. Maness, *Cyber Strategy: The Evolving Character of Power and Coercion* (Oxford: Oxford University Press, 2018).

[8] David E. Sanger, *The Perfect Weapon: War, Sabotage, and Fear in the Cyber Age* (New York: Broadway Books, 2019).

[9] David E. Sanger, "Obama Order Sped Up Wave of Cyberattacks Against Iran," *New York Times*, June 1, 2012, https://www.nytimes.com/2012/06/01/world/middleeast/obama-ordered-wave-of-cyberattacks-against-iran.html.

[10] David E. Sanger and Mark Mazzetti, "US Had Cyberattack Plan if Iran Nuclear Dispute Led to Conflict," *New York Times*, Feb. 16, 2016, https://www.nytimes.com/2016/02/17/world/middleeast/us-had-cyberattack-planned-if-iran-nuclear-negotiations-failed.html.

[11] Thomas Rid, "Cyber War Will Not Take Place," *Journal of Strategic Studies* 35, no. 1 (2012): 5–32, https://doi.org/10.1080/01402390.2011.608939; Adam P. Liff, "Cyberwar: A New 'Absolute Weapon'? The Proliferation of Cyberwarfare Capabilities and Interstate War," *Journal of Strategic Studies* 35, no. 3 (2012): 401–28, https://doi.org/10.1080/01402390.2012.663252; Julian Richards, *Cyber-War: The Anatomy of the Global Security Threat* (New York: Palgrave Pivot, 2014); Valeriano, Jensen, and Maness, *Cyber Strategy*; Erik Gartzke, "The Myth of Cyberwar: Bringing War in Cyberspace Back Down to Earth," *International Security* 38, no. 2 (2013): 41–73, https://doi.org/10.1162/ISEC_a_00136; Timothy J. Junio, "How Probable Is CyberWar? Bringing IR Theory Back In to the Cyber Conflict Debate," *Journal of Strategic Studies* 36, no. 1 (2013): 125–33, https://doi.org/10.1080/01402390.2012.739561; and Martin C. Libicki, *Cyberdeterrence and Cyberwar* (Santa Monica, CA: Rand Corporation, 2009), https://www.jstor.org/stable/10.7249/mg877af.

trol. Specifically, actors can use cyber operations to disrupt early-detection radar sites, allowing their military to approach undetected, or they can use cyber operations to disrupt command-and-control systems, making military operations more efficient and effective. Actors can also seek to flood their opponent's cellular phone systems with calls and text messages to prevent these systems from being used for effective communication on the battlefield.[12] Additionally, they can use malicious code to damage or compromise military infrastructure, making it ineffective and thereby disrupting battlefield command and control.

By contrast, information operations do not directly affect the battlefield, but can nevertheless indirectly influence military operations by undermining an adversary's support base and shaping perceptions of events. For instance, Russian government-sponsored hackers extensively used cyber and information operations to complement Kremlin military operations during its 2008 war in Georgia.[13] Weeks before the Russian invasion, several Georgian governmental websites were either taken down or displayed pro-Kremlin propaganda. During the five-day war, key sections of Georgia's internet servers were under the external control of Russian hackers.[14] These actions, deployed in conjunction with tactics used in military operations, aimed to make Russia's victory swift and decisive.[15]

Cyber Conflict as an Independent Tool

Outside the realm of cyber operations, there are abundant examples of various warfare technologies being used to complement and substitute for more traditional operations. For instance, during Operation Desert Storm — the U.S.-led campaign to recapture Kuwait in response to the Iraqi invasion — strikes by Apache attack helicopters were used as both a substitute for and complement to more traditional bombing runs by fixed-wing aircraft, which retain the relative strengths of greater range and payload. Apache helicopters carried out "surgical" attacks that disabled Iraqi early-warning radar sites, allowing coalition fixed-wing aircraft to approach Iraqi targets undetected and minimizing "collateral damage." It is thus not unreasonable to imagine that the increasing potential for harm through virtual conflict could enhance or replace more traditional modes of political aggression and defense.

However, despite scattered individual instances of substitution and/or complementarity, pundits' predictions on this score have largely not come to pass. In a recent study, we examined whether cyber operations mostly serve as complements to, or substitutes for, conventional conflict, or whether the two forms of conflict are more often exercised independently.[16] Our statistical analysis of global conventional military and cyber campaigns conducted by rivals between 2000 and 2010 suggests that cyber operations are generally not being used as either complements to or substitutes for conventional military operations.[17] Instead, countries tend most often to use these two types of operations independently from each other, due both to the difficulty of coordinating these modes of conflict and to the different strategic goals of each mode. For these reasons, our findings suggest, we have yet to witness the systematic use of cyber operations in a manner that is clearly coordinated and designed either to supplant or to further the traditional physical means and ends of conventional battle.

Tactically, force synchronization is difficult to achieve across domains. To execute an attack, an actor needs to find an exploitable vulnerability in a system or network. Given that this process takes significant time, it becomes quite difficult to coordinate its development with what is happening on the ground, making its use as a complement to traditional warfare challenging.[18] In addition, substitution is difficult to achieve because the different domains (cyber and conventional) are each better suited to achieving distinct objectives. Cyber operations are most effective in pursuing informational goals, such as gathering intelligence, stealing technology, swaying public opinion, or winning diplomatic debates. In contrast, a nation that covets a neighbor's territory, seeks to plunder natural resources, wishes to

[12] 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, https://doi.org/10.1177%2F0022002717737138.

[13] David Hollis, "Cyberwar Case Study: Georgia 2008," *Small Wars Journal*, Jan. 6, 2011, https://smallwarsjournal.com/blog/journal/docs-temp/639-hollis.pdf.

[14] Gregg Keizer, "Cyber Attacks Knock Out Georgia's Internet Presence," *Computerworld*, Aug. 11, 2008, https://www.computerworld.com/article/2532289/cyberattacks-knock-out-georgia-s-internet-presence.html.

[15] Richard G. Zoller, *Russian Cyberspace Strategy and a Proposed United States Response*, Army War College, 2010, https://apps.dtic.mil/sti/pdfs/ADA522027.pdf.

[16] Kostyuk and Gartzke, "Fighting in Cyberspace."

[17] As we explain, "Rivalries are ideal for this purpose, since they involve pairs of nations with demonstrated hostility, but that may or may not fight in a given time period." Kostyuk and Gartzke, "Fighting in Cyberspace," 17. We focus on this period due to the data availability.

[18] Kostyuk and Zhukov, "Invisible Digital Front."

hobble an enemy's military capabilities, or intends to terrorize a population or replace a political regime must still physically cross an adversary's borders in order to conquer or compel.

Given the difficulties of coordination and the lack of fungibility between actions and effects across domains, we argue — and report systematic evidence[19] — that cyber and conventional military operations operate largely independently, at least for now. As armies become better at synchronizing conflict across domains (i.e., multi-domain combat), cyber and traditional military operations may start to operate more as complements to one another in shaping battlefield dynamics.

The Indirect Link: Theory of Indirect Substitution

Though our research indicates that, for the time being, cyber warfare is more likely to be deployed independently from, rather than as a substitute for or complement to conventional warfare, it also indicates that a country's increased internet access is likely to lead to more cyber conflicts and less conventional conflict behavior. We label this effect "indirect substitution." This happens as a result of the following two circumstances.

First, cyberspace as a domain facilitates "useful" forms of international conflict. While information has been the focus of considerable attention and concern in warfare for centuries,[20] it became especially critical in the information age. Cyberspace is an environment in which adversaries seek out information about one another. Everyone is spying on everyone else, to discover intentions, to acquire knowledge, or to shape beliefs and thus behaviors. China has stolen both military and civilian industrial technology from the West through cyber operations.[21] Russia has used cyber operations to seek to influence the domestic politics of target nations.[22] The United States and perhaps Israel have used cyber attacks to counter Iranian efforts at nuclear proliferation.[23] In each case, the virtual domain was an extremely attractive space in which to operate, given these actors' objectives. While spies could have used physical means to obtain sensitive technologies or coerce opponents, these methods are costlier, riskier, and more difficult to conceal than cyber operations. Specifically, the bulk of traditional conventional military operations are not subtle, causing collateral or environmental damage and leaving an attacker open to international condemnation and possible retribution. As a result, cyber operations can be cheaper and more attractive than conventional tools of conflict, allowing an attacker to rebalance power anonymously.[24]

Second, traditional conflict domains are no longer adequate to achieve some of modern competitors' most important aims, which have shifted from acquiring land to acquiring information. For much of history, more land meant more wealth, which translated into the productive and destructive capacity of states. Today, much more of this capacity rests with human and financial capital. This transition in the motivation of states to pursue different aims has begun to transform international conflict. With the decline in the value of territory as a means of achieving wealth and power, the utility of conventional force has also declined, at least in its most traditional forms. The global spread of the internet has increased the need to acquire and control information. Information is power, especially in the information age. As a result, increasingly, contestation is occurring over the control of information, because of the increase in the value of information relative to other goods, such as territory or industrial equipment and facilities. Conventional military operations do not always provide an advantage over cyber operations for actors seeking to acquire or control information.

Before we apply our findings to explain Russia's actions in Ukraine, it is important to note that our analysis presents an overall relationship between cyber and military operations and does not focus on explaining individual cases. Extensively covered by prior research, these cases do not bear directly on our findings because they present behaviors that prove to be exceptions to prevailing patterns

[19] Kostyuk and Gartzke, "Fighting in Cyberspace."

[20] Geoffrey Blainey, *The Causes of War*, 3rd ed. (New York: The Free Press, 1988); and James D. Fearon, "Rationalist Explanations for War," *International Organization* 49, no. 3 (Summer 1995): 379–414, https://www.jstor.org/stable/2706903.

[21] Dan Blumenthal and Linda Zhang, "China Is Stealing Our Technology and Intellectual Property. Congress Must Stop It," *National Review*, June 2, 2021, https://www.nationalreview.com/2021/06/china-is-stealing-our-technology-and-intellectual-property-congress-must-stop-it/.

[22] "Russian Interference in 2016 U.S. Elections," Federal Bureau of Investigation, accessed Sept. 30, 2018, https://www.fbi.gov/wanted/cyber/russian-interference-in-2016-u-s-elections.

[23] Sanger, *The Perfect Weapon*.

[24] A parallel logic has led to the evolution of "gray-zone warfare," low-intensity conventional conflict designed to achieve objectives that cannot be pursued effectively in cyberspace, but which are also problematic in terms of the consequences of large-scale conventional war. See, Andres Gannon, et al., "The Shadow of Deterrence: Why Capable Actors Engage in Conflict Short of War," Draft, Jan 11, 2021, https://peterschram.com/wp-content/uploads/2021/01/gray_zone_web.pdf; and J. Andres Gannon, et al., "Why Did Russia Escalate Its Gray Zone Conflict in Ukraine?" *Lawfare*, Jan. 16, 2022, https://www.lawfareblog.com/why-did-russia-escalate-its-gray-zone-conflict-ukraine.

and not a general rule.[25] Despite that, the basic logic of complementarity and substitution in military affairs remains compelling, even if we do not find that it is exercised systematically in cyberspace, at least not yet. While we might see more systematic complementary and substitutive use of cyber and military operations in the future, we also expect that increasing global reliance on the internet, and the rising relative value of information, will continue to motivate countries to use cyberspace to strategically pursue information-related objectives independently of conventional military aims.

Russia's Cyber and Military Actions in Ukraine

While numerous details remain obscure in the midst of any war, consensus opinion seems to be that no major cyber operation has successfully disrupted any essential services in Ukraine during the period of the war. For the most part, Ukraine's internet infrastructure has remained functional despite the ongoing conflict. There is, however, no doubt that Russian hackers have sought to penetrate Ukrainian networks and will continue collecting intelligence to further Russia's strategic objectives. Moreover, the Russian government has been waging a vigorous series of information campaigns against occupied and free Ukrainian territory, as well as the rest of the world.[26] Why is this the case? What is the role of Russia's cyber efforts in this conflict? Is it using cyber operations to substitute for, complement, or operate independently from military operations?

Substitution

Advocates of the substitution argument have suggested that Russia would not need to use military force in Ukraine because cyber attacks would achieve similar goals. In effect, Russia would cross the border into Ukraine virtually, rather than physically, substituting cyber war for conventional conflict. Keir Giles of Chatham House, for example, argued that "a destructive cyber onslaught could target military command and control systems or civilian critical infrastructure and pressure Kyiv into concessions and its friends abroad into meeting Russia's demands."[27] A senior Biden administration official also espoused this logic, arguing that Russia "could opt to launch a sweeping cyber and disinformation campaign against Ukraine and its government rather than a traditional military invasion of the country."[28]

Some cyber attacks did take place while NATO and some of its member countries were still trying to negotiate a peaceful resolution of the crisis. These attacks suggested to informed observers that the Kremlin was more serious about cyber aggression than a physical invasion — perhaps to put pressure on NATO and Ukraine to accept some of its demands, thereby obviating military incursion.[29] In January of 2022, for instance, cyber operations defaced 70 Ukrainian websites.[30] Two days later, Microsoft identified the WhisperGate malware — a "pseudo ransomware"[31] — on computer systems belonging to Ukrainian government agencies, the purpose of which was to corrupt the contents of files on the computers it infected.[32] In February, cyber disruptive operations targeted PrivatBank, Ukraine's largest commercial bank,[33] and

[25] For instance, although one of the most active cyber attackers, North Korea is rarely a target of cyber operations, given its low levels of internet access. Travis Sharp, "Theorizing Cyber Coercion: The 2014 North Korean Operation Against Sony," *Journal of Strategic Studies* 40, no. 7 (2017): 898–926, https://dx.doi.org/10.1080/01402390.2017.1307741.

[26] Obviously, we cannot comment upon events that are unknown to us. While we have sought to anticipate what could be happening in cyberspace, our description of cyber operations is not without limitations. It is entirely possible that additional attacks might be occurring covertly. Some of these may come to light in the future. Given the delay between this manuscript submission and publication, we would also like to note that our brief review of cyber operations ends in early April. While some new cyber events either came to light or took place between early April and mid-June, they have not changed our main conclusions.

[27] Keir Giles, "Putin Does Not Need to Invade Ukraine to Get His Way," Chatham House, Dec. 6, 2021, https://www.chathamhouse.org/2021/12/putin-does-not-need-invade-ukraine-get-his-way.

[28] Martin Matishak, "Russia Could Launch Digital Offensive Against Ukraine, Administration Official Warns," *The Record*, Dec. 6, 2021, https://therecord.media/russia-could-launch-digital-offensive-against-ukraine-administration-official-warns.

[29] "The Hybrid War that Began Before Russia Invaded Ukraine," *Deutsche Welle*, Feb. 24, 2022, https://www.dw.com/en/hybrid-war-in-ukraine-began-before-russian-invasion/a-60914988.

[30] Kim Zetter, "What We Know and Don't Know About the Cyberattacks Against Ukraine - (Updated)," *Zero Day*, Jan. 17, 2022, https://zetter.substack.com/p/what-we-know-and-dont-know-about?s=r.

[31] Christiaan Beek, Max Kersten, and Raj Samani, "Return of Pseudo Ransomware," *Trellix*, Jan. 20, 2022, https://www.trellix.com/en-us/about/newsroom/stories/threat-labs/return-of-pseudo-ransomware.html.

[32] "Destructive Malware Targeting Ukrainian Organizations," Microsoft Threat Intelligence Center, Jan. 15, 2022, https://www.microsoft.com/security/blog/2022/01/15/destructive-malware-targeting-ukrainian-organizations/.

[33] Jenna McLaughlin "Ukraine Says Government Websites and Banks Were Hit with Denial of Service Attack," *NPR*, Feb. 15, 2022, https://www.npr.org/2022/02/15/1080876311/ukraine-hack-denial-of-service-attack-defense.

the websites of the Ukrainian Ministry of Defense and armed forces.[34]

However, if Moscow had used cyber operations to substitute for military operations, we should have seen a full-blown cyber war instead of a conventional invasion. The objective of Russia's pre-invasion cyber operations remains unclear. Even taken collectively, they resulted in modest damage and seemed to be rushed or poorly planned. For instance, the impact of web-defacement attacks was largely inconsequential, because most websites were quickly restored, and no data was lost or rendered unusable.[35] Microsoft discovered WhisperGate before it could cause serious damage.[36] PrivatBank restored its services within hours.[37] Ukrainian officials reported no significant damage to the websites of the Ukrainian Ministry of Defense and armed forces.[38] Though Russia has apparently tried, over the last eight years, to use cyber operations to supplant its conventional front,[39] Moscow's limited cyber efforts in the period immediately prior to the invasion suggest that it recognized the futility of such efforts. While a systematic analysis of the relationship between Russia's cyber and military operations is in order, it appears that, having failed to achieve its strategic objectives using cyber operations, the Kremlin perceived that its only option was to launch a military campaign.[40]

Complementarity

Rather than act as a substitute, other observers and pundits have argued that cyber operations may be used to complement conventional military operations in a Russian assault on Ukraine. Jason Healey of Columbia University predicted that Russia would

[34] Yuras Kurmanau and Frank Bajak, "Ukrainian Army, Major Banks Hit by Cyberattacks as Russian Military Threat Looms," *Global News*, Feb. 15, 2022, https://globalnews.ca/news/8622244/ukraine-military-government-sites-cyberattack/.

[35] Zetter, "What We Know and Don't Know."

[36] Microsoft Threat Intelligence Center, "Destructive Malware Targeting Ukrainian Organizations."

[37] McLaughlin "Ukraine Says Government Websites and Banks Were Hit with Denial of Service Attack."

[38] Kurmanau and Bajak, "Ukrainian Army, Major Banks Hit by Cyberattacks as Russian Military Threat Looms."

[39] Lennart Maschmeyer and Nadiya Kostyuk, "There Is No Cyber 'Shock and Awe': Plausible Threats in the Ukrainian Conflict," *War on the Rocks*, Feb. 8, 2022, https://warontherocks.com/2022/02/there-is-no-cyber-shock-and-awe-plausible-threats-in-the-ukrainian-conflict/.

[40] Maschmeyer and Kostyuk, "There Is No Cyber 'Shock and Awe.'"

initiate any invasion of Ukraine with offensive cyber attacks.[41] William Courtney and Peter A. Wilson from the RAND Corporation warned of the "massive employment" of cyber operations to create "shock and awe causing Ukraine's defenses or will to fight to collapse."[42] A report from Microsoft Corporation published in April of 2022 seemed to substantiate these claims of the complementary use of cyber and military campaigns, at least at first blush.[43]

Cyber attacks that took place during the NATO-Russia-Ukraine negotiations — some of which are outlined above — could have suggested that Moscow was planning to unleash congruent, complementary cyber Armageddon as it crossed the Ukrainian border with tanks.[44] Moreover, a number of cyber disruption and degradation attacks followed Russia's invasion of Ukraine, hinting at their potential complementary use alongside Russia's military campaigns. For instance, on February 24, the start date of Russia's invasion, large parts of Viasat's KA-SAT network of high-speed satellite services went down,[45] causing a partial outage in its residential broadband services in Ukraine and in other European countries[46] (thousands of wind turbines in Germany were forced offline by the outage).[47] The heavy reliance of the Ukrainian military on the compromised KA-SAT segment in Central and Eastern Europe led German government officials to associate the cyberattack on Viasat with the war in Ukraine.[48] On March 17, 2022, the Ukrainian government and military entities were targeted using spear-phishing campaigns — e-mails containing malicious files with the purpose of obtaining access to information available to these entities.[49] On March 28, 2022, Ukraine's national provider Ukrtelecom experienced a major internet disruption due to a cyberattack, with its connectivity collapsing to only thirteen percent of pre-war levels.[50]

But as with cyber strikes prior to the invasion, the strategic impact of these attacks remained relatively minor, suggesting that the Russian government had not expected these cyber operations to significantly complement its actions on the ground. The German federal government characterized the effect of the attacks on Viasat's KA-SAT network as a case of "cyber collateral damage"; there were no further effects on German critical infrastructure or on Germany's ability to provide for its security.[51] In the aftermath of the above-listed cyber attacks, Ukrtelecom was able to quickly resume regular services.

Even though the impact of cyber operations seems to be limited given the scale of the full-blown conventional war, it is quite possible that a greater number of attacks might eventually come to light. Still, even if much of the goings-on in cyberspace occur behind the scenes, there is clearly little support for claims that cyber operations are being conducted in a direct, overt manner to impact the reality of combat on the ground. Had we witnessed cyber operations that misdirected enemy forces, confounded the disposition of forces, or damaged or immobilized equipment, especially high-tech electronics systems (ELINT, etc.), we would of course have to conclude otherwise.

Independence

Having detailed the failure of the Russian government to implement cyber operations either to complement or substitute for military operations, we next apply our study's findings to show how the Kremlin has used its cyber and conventional capabilities independently of each other.

One of the reasons for this independence, as noted above, is the difficulty of coordinating operations across domains, a known challenge even for

[41] Healey, "Preparing for Inevitable Cyber Surprise."

[42] Courtney and Wilson, "If Russia Invaded Ukraine."

[43] "Special Report: Ukraine, An Overview of Russia's Cyberattack Activity in Ukraine," Microsoft, April 27, 2022, https://query.prod.cms.rt.microsoft.com/cms/api/am/binary/RE4Vwwd.

[44] Maggie Miller, "The World Holds Its Breath for Putin's Cyberwar," *Politico*, March 23, 2022, https://www.politico.com/news/2022/03/23/russia-ukraine-cyberwar-putin-00019440.

[45] Michael Sheetz, "Viasat Believe 'Cyber Event' Is Disrupting Its Satellite-Internet Service in Ukraine," *CNBC*, Feb. 28, 2022, https://www.cnbc.com/2022/02/28/ukraine-updates-viasat-says-cyber-event-disrupting-satellite-internet-service.html.

[46] Eva Mathews, "Satellite Firm Viasat Probes Suspected Cyberattack in Ukraine and Elsewhere," *Reuters*, Feb. 28, 2022, https://www.reuters.com/business/aerospace-defense/satellite-firm-viasat-probes-suspected-cyberattack-ukraine-elsewhere-2022-02-28/.

[47] Von Svea Eckert and Hakan Tanriverdi, "Cyberattacken Als Rache Für Sanktionen?" *Tagesschau*, March 3, 2022, https://www.tagesschau.de/investigativ/russland-cyberattacken-105.html.

[48] "Satellitennetzwerk Viasat Offenbar Gezielt in Osteuropa Gehackt," *Der Spiegel*, March 5, 2022, https://www.spiegel.de/netzwelt/web/viasat-satellitennetzwerk-offenbar-gezielt-in-osteuropa-gehackt-a-afd98117-5c32-4946-ab8a-619f1e7af024.

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

[50] "Ukraine: Timeline Of Cyberattacks on Critical Infrastructure and Civilian Objects," CyberPeace Institute, updated June 8, 2022, https://cyberpeaceinstitute.org/ukraine-timeline-of-cyberattacks/.

[51] *Der Spiegel*, "Satellitennetzwerk Viasat Offenbar Gezielt in Osteuropa Gehackt."

the most sophisticated militaries.[52] Cyber attacks are generally more planning intensive than conventional operations because they require significant time and resources to conduct reconnaissance to determine which vulnerabilities an actor can exploit.[53] Having exploited a given vulnerability, the actor has to start the process all over again. By contrast, in the case of conventional military tools, once an actor has started shooting it can continue shooting as long as it has available ammunition.

Russian military actions in Ukraine show that Russia's forces are having difficulty coordinating, even within a single domain.[54] Moreover, since there is anecdotal evidence suggesting that the Kremlin expected the war in Ukraine to be of short duration,[55] Moscow might not have prepared its forces to execute time-intensive cyber operations to complement its actions on the ground. As a result, Russian commanders would have had little choice but to employ conventional military operations to seek to capture, damage, or destroy critical infrastructure. That could be one reason why, for example, Russian officials relied exclusively on conventional military operations to capture the Zaporizhzhia nuclear power plant, which generates more than one-fifth of Ukraine's total electricity. And, as demonstrated by the 2015 and 2016 attacks on Ukraine's electric power grid, which led to power outages that lasted only a few hours, the potentially limited strategic impact of infrastructure-targeted cyber operations might also help explain Russia's reliance on conventional military operations in the current campaign.[56]

Moreover, the gains of using disruptive and degrading cyber attacks as complements are lower than their costs. Ukraine's decentralized internet, which includes multiple fiber lines that cover the same areas, makes it difficult to effectively attack Ukraine's network connectivity.[57] In addition, Russian forces in Ukraine have utilized the well-connected Ukrainian commercial networks for their own battlefield communications.[58] Finally, if the Kremlin were to succeed in conquering Ukraine, it would be expensive to rebuild the country's internet infrastructure. In civil conflicts across the globe, governments and nonstate actors both rely on cellular communications. As a result, both are inclined to leave cell towers and other vulnerable infrastructure alone. There is little evidence that Russia is using disruptive and degrading cyber attacks to complement ground operations, in part because such attacks would also degrade Russia's own efforts to maintain communication, now and in the future. This lack of evidence of the complementary use of disruptive and degrading cyber attacks and military operations provides preliminary support for the independence of these modes of fighting. This suggests that each tends to operate in its own bubble — the findings demonstrated in our global analysis as well as in research that investigated the role of these operations during the earlier stage of the Ukraine conflict between 2014 and 2016.[59]

Another reason why we do not observe complementarity between Russia's known cyber attacks and military operations might be because it is more valuable to Moscow to use the internet to eavesdrop on the conversations of the Ukrainian military and civilian population, in order to gather information about the territory and to geolocate objectives, than it is to take the internet offline.[60] Cyber espionage may assist the Kremlin in obtaining Ukrainian battle plans in order to better execute its military campaigns and target valuable objects, or assist in meeting even more basic needs like navigation. There is evidence that Russian forces — supplied with only rudimentary GPS capabilities and outdated, inaccurate paper maps — have relied on Google Maps and other internet-based geographical infor-

[52] Kostyuk and Zhukov, "Invisible Digital Front."

[53] Rowland Manthorpe, "Will Russia Launch a Cyberattack on the West?" *Sky News*, March 15, 2022, https://www.dw.com/en/hybrid-war-in-ukraine-began-before-russian-invasion/a-60914988.

[54] Gustav Gressel, "Combined Farces: Russia's Early Military Failures in Ukraine," European Council on Foreign Relations, March 15, 2022, https://ecfr.eu/article/combined-farces-russias-early-military-failures-in-ukraine/.

[55] Aaron Schaffer, "Ukraine Suffered Two Cyberattacks in the Lead-Up to Russia's Invasion," *Washington Post*, March 30, 2022, https://www.washingtonpost.com/politics/2022/03/30/ukraine-suffered-two-cyberattacks-lead-up-russia-invasion/.

[56] 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/.

[57] Gerrit De Vynck, Rachel Lerman, and Cat Zakrzewski, "How Ukraine's Internet Still Works Despite Russian Bombs, Cyberattacks," *Washington Post*, March 29, 2022, https://www.washingtonpost.com/technology/2022/03/29/ukraine-internet-faq/.

[58] De Vynck, Lerman, and Zakrzewski, "How Ukraine's Internet Still Works."

[59] Kostyuk and Gartzke, "Fighting in Cyberspace"; and Kostyuk and Zhukov, "Invisible Digital Front."

[60] Sam Sabin and Laurens Cerulus, "Why Ukraine's Phones and Internet Still Work," *Politico*, March 7, 2022, https://www.politico.eu/article/why-ukraines-phones-and-internet-still-work/.

mation systems to find their way around.[61]

Since this information collected via the internet has benefitted the Kremlin, one might well argue that the Kremlin's cyber espionage operations are therefore complementing efforts on the battlefield. But it is important to note that cyber operations are not enhancing any of the physical effects of conventional warfare, for Ukraine or Russia. They are not, as predicted, being used in a coordinated manner to make either side more lethal on the battlefield. The explosion of artillery shells is not bigger. Tanks are not more immune to interdiction by precision-guided munitions such as the Javelin or NLAW. Nor does the availability of networks seem to be coordinated with battlefield conditions. If, for example, we accept for the moment that cyberspace is helping Ukrainian forces master the battlefield, then why would Russian commanders wish to allow this to continue? At the very least, the complementarity theory implies that Russia should shut down the internet, or cellular communications, when and where these systems become a tactical liability. This has not generally been the case. As a result, while there might be some individual cases of the complementary use of cyber and conventional operations for tactical purposes, both modes of fighting seem to be used independently from each other.

Another reason why cyber and conventional operations are being used independently of one another is that different political objectives require the use of disparate conflict domains to achieve various aims.[62] This also explains our indirect substitution argument, discussed below.

Indirect Substitution

As our theory explains, traditional military operations are the most effective method of occupying territory, capturing resources, attriting an enemy's conventional military capabilities, and terrorizing populations. Cyber operations, on the other hand, are most consistently effective in gathering intelligence, stealing technology, and winning public opinion and diplomatic debates. As a result, conflict in cyberspace has more typically been about winning information contests than it has been about augmenting or replacing the physical aspects of a conventional war, at least directly. As noted earlier, because of the unique objectives that each mode serves, they can instead act to *indirectly* substitute for one another. Existing evidence suggests that Russia has used its information campaigns to *indirectly substitute* for conventional conflict in the longer term, especially given that Moscow seems to have expected the war to be short.

During the invasion, the Russian government continued using the internet to shape the hearts and minds of Ukrainians and the rest of the world. The Kremlin launched a number of disinformation campaigns using compromised accounts of high-profile Ukrainians, including military officials and public figures.[63] As of the end of March 2022, for instance, the Security Service of Ukraine (SBU) had identified and shut down five bot farms operating 100,000 social media accounts spreading fake news related to the invasion.[64] Hackers broke into local government websites to spread false information that Kyiv had capitulated and had signed a peace treaty with Moscow.[65] Given that information campaigns are meant to shape public opinion in the long term, the Russian government might have been using these campaigns to indirectly substitute for fighting in the future.

Indirect Complementarity

While Russia has arguably used its information campaign to indirectly substitute for conventional conflict in the longer term, it may also have used information and cyber espionage operations to indirectly complement its conventional invasion in the short term.[66] Some experts have suggested that Russia has most likely been trying to retain access to information about decision-making processes not only of the government of Ukraine, but also of Western states. The Kremlin has tailored its cyber espionage activities in order to obtain information about Western governments' discussions of economic sanctions against Russia, how these governments

[61] Rachel Lerman, "On Google Maps, Tracking the Invasion of Ukraine," *Washington Post*, updated Feb. 27, 2022, https://www.washingtonpost.com/technology/2022/02/25/google-maps-ukraine-invasion/.

[62] Kostyuk and Gartzke, "Fighting in Cyberspace."

[63] Dan Milmo, "Facebook Takes Down Ukraine Disinformation Network and Bans Russian-Backed Media," *The Guardian*, Feb. 28, 2022, https://www.theguardian.com/technology/2022/feb/28/facebook-takes-down-disinformation-network-targeting-ukraine-meta-instagram.

[64] "З початку війни СБУ ліквідувала 5 ворожих ботоферм потужністю понад 100 тис. фейкових акаунтів," Sluzhba Bezpeky Ukraiinu, March 28, 2022, https://ssu.gov.ua/novyny/z-pochatku-viiny-sbu-likviduvala-5-vorozhykh-botoferm-potuzhnistiu-ponad-100-tys-feikovykh-akauntiv.

[65] Raphael Satter, "Ukrainians Say Hackers Used Local Government Sites to Spread Fake 'Capitulation' News," *Reuters*, March 3, 2022, https://www.reuters.com/world/europe/ukrainians-say-hackers-used-local-government-sites-spread-fake-capitulation-news-2022-03-03/.

[66] Our systematic research, which focuses on cyber operations and not information operations, shows indirect complementarity and not indirect substitution. Further research should explore the possibility of indirect complementarity between military and information operations on the global level.

work together to address Russia's invasion, and the types of divisions that the Kremlin might be able to exploit and use as leverage in future negotiations.[67]

Russia's extensive use of the internet to spread disinformation demonstrates that its other priority in cyberspace is to target the hearts and minds of domestic and international audiences. Prior to the start of the conflict, the Russian government had actively engaged in a number of disinformation campaigns aimed at shaping the beliefs of the Ukrainian population.[68] In November 2021, we observed a 2,000 percent daily average increase in Russian-language content about the situation in Ukraine.[69] At the time, White House Press Secretary Jen Psaki stressed the potential psychological effects of these operations by Moscow, which sought to make the case for Russia's intervention in Ukraine and to build support among Russian-speaking Ukrainians for a possible Russian invasion. Through these efforts, Russian officials hoped to exploit divisions in Ukraine to accelerate the march to Kyiv, and to smooth the installation of and transition to an anticipated pro-Kremlin regime.[70]

Note that, while using cyberspace in this manner changed important details of the eventual Russian invasion — streamlining the order of battle and convincing Putin and others in Moscow that they could prevail on the cheap — it did not obviate the need for an invasion. Sowing dissension in Ukraine would not have led to regime change by itself. Nor could the invasion prevail with only light force if a critical mass of citizens failed to greet the invaders with flowers. The information campaign and the invasion were intended to accomplish different things, one capturing hearts and minds, and the other grabbing territory. In other words, though each complemented the other, they did so separately, independently, and *indirectly*.

While our analysis does not point to indirect complementarity of cyber and conventional fronts on a global scale, Russia's actions in Ukraine suggest the possibility of this new relationship between these two types of operations in future digitally enabled conflicts. Future research should further explore this possibility.

Alternative Explanations for the Lack of Full-Blown Cyber Warfare in Russia's War Against Ukraine

A number of alternative arguments have emerged to explain why Russia has not engaged in full-blown cyber warfare in Ukraine. One argument focuses on Ukraine's cyber defenses, which may have been highly effective, perhaps as a result of cooperation between NATO countries and the Ukrainian government.[71] While it is perhaps an understandable generalization triggered by the notable successes of Ukrainian ground and air forces, this seems unlikely. While numerous unobserved Russian cyber attacks might have been thwarted behind the scenes by Ukrainian (or other) cyber defenders, the attacks that have been observed are less of a reflection of Ukrainian excellence than of Russian lethargy; Russia's lack of preparation; or Russia's lack of a desire, need, or intent to execute disruptive and degrading cyber attacks. Specifically, Russian cyber attacks undermined their targets only temporarily and seemed to have been hastily planned.[72] Moreover, given its access to Ukraine's networks, it seems most likely that the Kremlin has made a decision not to use that access to disrupt the internet and instead had decided to use access information, both in order to listen in and to spread disinformation.

A second alternative is that Russia may be holding some of its cyber assets in reserve and is waiting for the right moment to strike. This argument suggests that a major cyber onslaught may be in the offing that would act as a force multiplier to propel Russia's conventional military operations.[73] If so, then there could not have been a better time

[67] Pascale Davies, "Cyber Espionage Is Key to Russia's Invasion of Ukraine. The International Community Is Fighting Back," *Euronews*, updated March 9, 2022, https://www.euronews.com/next/2022/03/09/cyberespionage-is-key-to-russia-s-invasion-of-ukraine-the-international-community-is-fight.

[68] "Press Briefing by Press Secretary Jen Psaki and FEMA Administrator Deanne Criswell, January 14, 2022," The White House, Jan. 14, 2022, https://www.whitehouse.gov/briefing-room/press-briefings/2022/01/14/press-briefing-by-press-secretary-jen-psaki-and-fema-administrator-deanne-criswell-january-14-2022/.

[69] The White House, "Press Briefing by Press Secretary Jen Psaki and FEMA Administrator Deanne Criswell."

[70] Andrew E. Kramer, "Russia's Grave Miscalculation: Ukrainians Would Collaborate," *New York Times*, May 7, 2022, https://www.nytimes.com/2022/05/07/world/europe/russia-putin-ukraine-politicians.html.

[71] "NATO, Kiev to Sign Agreement on Enhanced Cyber Cooperation Within Days — NATO chief," *TASS*, Jan. 14, 2022, https://tass.com/world/1388351?utm_source=google.com&utm_medium=organic&utm_campaign=google.com&utm_referrer=google.com.

[72] Zetter, "What We Know and Don't Know."

[73] David E. Sanger, et al., "Arming Ukraine: 17,000 Anti-Tank Weapons in 6 Days and a Clandestine Cybercorps," *New York Times*, March 6, 2022, https://www.nytimes.com/2022/03/06/us/politics/us-ukraine-weapons.html.

Russia's extensive use of the internet to spread disinformation demonstrates that its other priority in cyberspace is to target the hearts and minds of domestic and international audiences.

to unleash this torrent from cyberspace than in the early weeks of the conflict, a period during which Russian forces suffered a prodigious level of casualties, failed to capture any of their putative objectives, and demonstrated significant incompetence as a military organization. If Russian hackers are holding back, waiting for a moment when they are really needed, it is unclear what needs to take place in order for them to be mobilized.

Since it takes significant time to build access and capabilities, which the Kremlin had not planned on using against a seemingly weak actor, the third possibility is that we can expect to see a more coordinated use of cyber operations along with military operations in the future. This, however, is unlikely to take place, given that the Russian government has been present in Ukraine's cyber infrastructure for the better part of a decade.[74] While it might not have access to every target of significant value, it is likely that Russia has access to more targets than it has damaged, disabled, or destroyed to date. The fact that Moscow has generally failed to exploit such vulnerabilities in a destructive manner, rather than in order to conduct espionage, suggests it does not see significant advantages in doing so.

The last possibility is that there is a lack of suitable targets. Many Ukrainian objects of critical infrastructure may not be connected to the internet. Much of Ukraine's military equipment, for example, is leftover from the Soviet era.[75] There is no point in seeking to attack, say, a radar site via the internet when the radar runs on vacuum tubes and the only cyber links are the operators' smartphones. Yet again, however, this does not explain the lack of cyber aggression where the environment is more target rich, either in Ukraine or the West. A limited target set implies that it is that much easier to achieve target saturation, something we have not seen come to pass four months into the war.

While there are many possible reasons for the limited nature of Russia's cyber war in Ukraine, the arguments outlined above suffer from various fairly obvious flaws. Russian hackers are probably not pulling their punches. More likely, as argued above, cyber war is deemed by the Kremlin to impede rather than enhance battlefield conditions. Attacks over the internet that are designed to damage or destroy are not nearly as attractive as maintaining access in order to collect information, shape perceptions, and gauge the effects of one's actions in other domains.

Lessons for the Future

The old Clausewitzian dictum still holds, even in the 21st century: Warfare is the continuation of politics, even by an increasing number of other means.[76] But the goals of politics are heterogeneous, and the means themselves differ in their efficaciousness, depending on the goal. Cyber war is first and foremost about information — its control and utilization as a means of realizing political goals.[77] Because it is primarily an informational domain, cyberspace is most useful in pursuing informational goals. In Ukraine, we can see that this is precisely what Russia is doing: using the internet to seek to shape the beliefs of Ukrainian citizens and perhaps also to glean better insights about the conduct of the war and order of battle, both in practice (i.e., against Ukraine) and in prospect (i.e., against NATO and the West generally).

Hollywood has gotten cyber war wrong, preferring to imagine a domain in which bits and bytes somehow lead to spectacular explosions.[78] Intellectuals have not done much better. Rather than looking for direct, palpable effects, we are better off considering how information shapes political affairs indirectly and how politicians seek to condition information. Cyber war is more about beliefs and data than it is about wresting physical control over objects or destroying material capabilities.

What can we expect from cyberspace in future wars? Most likely, more of the same. The Russo-Ukrainian conflict has already demonstrated tendencies that we identified in a more systematic analysis. Cyber attacks do not generally lead to increased conventional conflict behavior. Nor does cyber war make redundant conflict in other domains. Instead, there has been a decline in conventional war, brought on by the diminishing utility of controlling tangible goods. Taking territory is no longer the fast route to wealth and power that it once was. Instead, important nations collect, contain, and ac-

[74] Donghui Park and Michael Walstrom, "Cyberattack on Critical Infrastructure: Russia and the Ukrainian Power Grid Attacks," The Henry M. Jackson School of International Studies, Oct. 11, 2017, https://jsis.washington.edu/news/cyberattack-critical-infrastructure-russia-ukrainian-power-grid-attacks/.

[75] Alex Horton, Claire Parker, and Dalton Bennett, "On the Battlefield, Ukraine Uses Soviet-Era Weapons Against Russia," *Washington Post*, April 29, 2022, https://www.washingtonpost.com/world/2022/04/29/urkaine-russian-soviet-weapons/.

[76] Carl von Clausewitz, "On War," in *On War*, ed. and trans. Michael Howard and Peter Paret (Princeton, NJ: Princeton University Press, 2008).

[77] Robert Chesney, et al., "Policy Roundtable: Cyber Conflict as an Intelligence Contest," *Texas National Security Review*, Sept. 17, 2020, https://tnsr.org/roundtable/policy-roundtable-cyber-conflict-as-an-intelligence-contest.

[78] Myriam Dunn Cavelty, *Cyber-Security and Threat Politics: US Efforts to Secure the Information Age* (Abingdon, UK: Routledge, 2008).

quire knowledge. The ability to build sophisticated technologies and glean and process insights about one another differentiates powerful nations from those that can only wish to be so. These diverging objectives point to the possibility of indirect substitution of the two modes of fighting.

The Russo-Ukrainian war has been a surprise in many ways. Few observers expected a major European conflict in the 21st century. Most experts vastly over-estimated the efficacy of the Russian army and perhaps under-estimated the fighting spirit and acumen of Ukrainian forces. Yet another surprise has been the relative lack of combat in the cyber domain. However, we anticipated this particular tendency in our explanation of the independence of cyber and conventional domains. The war in Ukraine is fundamentally about territory and physical control. Cyberspace can do little to capture a nation. It can, however, serve as a vehicle through which one can attempt to capture the hearts and minds of a people. But to compete in this manner, both sides must maintain access to the internet.

It is quite possible that in the future other nations will behave differently than Russia has in Ukraine. Despite this, our systematic analysis of global military and cyber campaigns and descriptive anecdotes from the Russo-Ukrainian war suggest that cyber war cannot replace traditional forms of combat. Cyber attacks will also often fail to make physical attacks more effective or practical, unless and until each is well coordinated with the other. Even then, it will make little sense to coordinate across domains unless each domain is utilized for its primary purposes. Breaking things over the internet is hard work and not very productive in political terms. Much more can be done by collecting and disseminating (dis)information in cyberspace, which can then be used to enhance outcomes in other domains. Differences in these respective arenas mean that the future of warfare will likely not be fundamentally altered by cyberspace. Instead, the objectives of states are already evolving in an informational world. Nations will not use cyber war in the place of more traditional war, but they will rely increasingly on cyberspace as a domain for pursuing these new, informational objectives.

Dr. Nadiya Kostyuk *is an assistant professor at the School of Public Policy and the School of Cybersecurity and Privacy at Georgia Institute of Technology. Her research focuses on security studies, modern warfare, cyber conflict, cyber institutions and capability, and Russian and Eurasian politics. Dr. Kostyuk's research has been published (or is forthcoming) in the* Journal of Peace Research, *the* Journal of Conflict Resolution, *the* Journal of Global Security Studies, *the* Journal of Strategic Security, *the* Institute of Electrical and Electronics Engineers (IEEE), *the* Cyber Defense Review, *and several edited volumes and general-audience publications. Dr. Kostyuk is a director of the Cybersecurity Summer Institute and is a co-organizer (with Christopher Whyte) of the Digital Issues Discussion Group. From 2013 to 2014, Dr. Kostyuk served as a program coordinator for the Global Cooperation in Cyberspace Initiative at the EastWest Institute (EWI). From 2014 to 2020, Dr. Kostyuk served as a cyber security fellow in the same initiative. During her time at EWI, Dr. Kostyuk participated in various Track 1.5-2 dialogues between Russian and U.S. counterparts on the topic of cyber security.*

Dr. Erik Gartzke *is a professor in the Department of Political Science at the University of California, San Diego. Professor Gartzke studies the impact of information on war, peace, and international institutions. Professor Gartzke's research has appeared in the* American Journal of Political Science, International Organization, International Studies Quarterly, *the* Journal of Conflict Resolution, *the* Journal of Politics, *and elsewhere. He is currently working on two books, one on globalization and the other on the democratic peace, as well as dozens of articles. Dr. Gartzke founded and directs the Center for Peace and Security Studies (cPASS), which has conducted roughly $15 million in sponsored policy-relevant research for entities like the U.S. Department of Defense, the Office of the Director of National Intelligence, the Defense Threat Reduction Agency, and other agencies.*

Acknowledgments*: Andres Gannon and Ryan Shandler provided helpful comments on the earlier drafts of this article.*

Image: Ministry of Defense of Ukraine (CC BY-SA 2.0)[79]

[79] For the image, see https://www.flickr.com/photos/140624011@N02/26920250611. For the license, see https://creativecommons.org/licenses/by-sa/2.0/.