Russian Cyber Operations in the Invasion of Ukraine

Dr. Herbert Lin

INTRODUCTION

In March 2021, Russia began to deploy large numbers of troops and armaments near the Russia-Ukraine border in what Western observers believed posed an invasion threat to Ukraine, which Russia strongly denied. An intense debate in the West ensued over whether the troops were being deployed to pressure Ukraine into making political concessions or to conduct an actual invasion.

Noting previous Russian offensive cyber operations against Ukraine starting as early as 2014, many cyber analysts and scholars predicted that an invasion would be accompanied by significant cyberattacks on Ukraine and possibly on Western nations supporting Ukraine, including particularly the US. For example, Maggie Miller wrote in *Politico* that "in a full-scale cyber assault [on Ukraine], Russia could take down the power grid, turn the heat off in the middle of winter and shut down Ukraine's military command centers and cellular communications systems."[1] Samuel Charap of the RAND Corporation thought the most likely Russian response to Western economic sanctions would be a cyber operation that temporarily shut down some major Western banks.[2]

Russia launched its invasion of Ukraine on February 24, 2022. Since then, many cyber analysts and scholars have observed that Russian offensive cyber operations have played a relatively small role compared to its kinetic operations. For example, in explaining why Russian cyber operations had yet to play an important tactical role in its invasion, Nadiya

Dr. Herbert Lin is senior research scholar for cyber policy and security at the Center for International Security and Cooperation and Hank J. Holland Fellow in Cyber Policy and Security at the Hoover Institution, both at Stanford University. His research interests relate broadly to policy-related dimensions of cybersecurity and cyberspace, with particular focus on the use of offensive operations in cyberspace as instruments of national policy and security dimensions of information warfare and influence operations on national security. He is also Chief Scientist Emeritus for the Computer Science and Telecommunications Board, National Research Council (NRC) of the National Academies, where he served (1990-2014) as study director of major projects on public policy and information technology, and Adjunct Senior Research Scholar and Senior Fellow in Cybersecurity (not in residence) at the Saltzman Institute for War and Peace Studies in the School for International and Public Affairs at Columbia University. In 2016, he served on President Obama's Commission on Enhancing National Cybersecurity.

Kostyuk and Erik Gartzke argued that that such operations were best suited for pursuing informational goals, such as gathering intelligence, stealing technology, or winning public opinion or diplomatic debates, whereas kinetic military operations occupy territory, capture resources, diminish the military capability of opponents, and terrorize populations.[3] Writing with Lennart Maschmeyer,[4] Kostyuk poses an important question: If cyber operations offer effective and potent instruments for coercion, why did Russia go to the effort and expense of mobilizing its troops? Their conclusion is that cyber operations do not in fact provide such instruments.

On April 12, 2022, the Ukrainian Computer Emergency Response Team (CERT-UA) and the Slovakian cybersecurity firm ESET issued advisories that the Sandworm hacker group, confirmed to be Unit 74455 of Russia's military intelligence agency, the GRU, had conducted cyberattacks against high-voltage electrical substations in Ukraine,[5] which reportedly were thwarted but could possibly have hit two million Ukrainians with lost power. (An earlier, private advisory from CERT-UA reported that power to nine electrical substations had been temporarily switched off, but this later was disavowed by Victor Zhora, Ukraine's deputy head of the State Special Service for Digital Development, characterizing the private report as "preliminary," and a "mistake."[6])

Russia was not entirely inactive on the cyber front. For example, on the first day of the invasion, a Russian cyberattack on tens of thousands of satellite modems in Ukraine and elsewhere in Europe disabled Internet service for many in those regions. Going beyond a simple denial-of-service attack, this attack also destroyed key data on these modems, rendering them permanently inoperative. A Ukrainian cyber official said the attack led to "a really huge loss in communications in the very beginning of the war,"[7] although one more recent report indicates that this official's comments regarding the magnitude of the impact were misunderstood

at the time.[8] Other cyberattacks conducted contemporaneously with or just prior to the invasion include the following:

- Ukrainian websites across multiple sectors were subjected to Russian distributed denial-of-service (DDoS) attacks in mid-February, including one on the Ukrainian Ministry of Defense on February 15.[10]
- Russian wiper malware programs appeared in Ukrainian systems; to date, a number of distinct variants have been identified. These programs erase user data, programs, and hard drives.[11] Wiper malware-affected Ukrainian government, financial, information technology, and energy sectors also spread to systems in other European countries.
- Ukrainian Internet services were temporarily disrupted in targeted attacks on telecommunications providers Triolan on March 9, Vinasterisk on March 13, and Ukrtelecom on March 28.[12]
- A month into the invasion, Russia launched cyberattacks against Starlink terminals, which SpaceX had deployed into Ukraine to augment its satellite communications capability. These attacks reportedly succeeded for several hours, until SpaceX updated software to resist such attacks.[13]
- Western social media companies identified several disinformation campaigns. These campaigns have included coordinated inauthentic behavior on social media, brief takeovers of media channels, and attempts to compromise social media accounts.[14] On March 28, the Security Service of Ukraine announced that it had shut down five disinformation-spreading bot farms operating over 100,000 social media accounts since the invasion began.[15]

Implicitly building on these examples, David Cattler and Daniel Black, Assistant Secretary General for Intelligence and Security and Principal Analyst in the Cyber Threat Analysis Branch at NATO, respectively, wrote in *Foreign Affairs* that "the magnitude of Moscow's pre-kinetic destructive cyber-operations was unprecedented" and that on February 24, 2022, "Russian cyber-units successfully deployed more destructive malware—including against conventional military targets such as civilian communications infrastructure and military command and control centers—than the rest of the world's cyberpowers combined typically use in a given year." They assert that, contrary to assessments that Russian cyber operations were ineffective, Russia's invasion strategy "failed to capitalize on the full capabilities and numerous operational successes of its cyber-units." They further argue that "cyber operations have been Russia's biggest military success to date in the war in Ukraine," and that "they will continue to provide Moscow a flexible tool capable of hitting a range of targets in Ukraine and beyond."[16]

Microsoft has compiled the most complete inventory of cyberattacks against Ukraine to date,[17] reporting that "the cyber operations so far have been consistent with actions to degrade, disrupt, or discredit Ukrainian government, military, and economic functions, secure footholds in critical infrastructure, and to reduce the Ukrainian public's access to information." Microsoft

observed that "cyber and kinetic military operations appeared to be directed toward similar military objectives. Threat activity groups often targeted the same sectors or geographic locations around the same time as kinetic military events." However, it was unclear "if there was coordination, centralized tasking or merely a common set of understood priorities driving the correlation."

Assuming this listing captures most cyberattacks immediately before the invasion and thereafter (see below note for a type of cyberattack that was not captured), the timeline suggests that cyber activity against Ukraine increased post-invasion but to a lesser degree than what many commentators expected. Thus, while Russia has enjoyed some degree of success in cyberspace in prosecuting its invasion, its cyber operations have fallen short of many experts' pre-invasion predictions.

This lack of impact has characterized both strategic and tactical dimensions of the conflict. Strategically, Russian cyberattacks have not affected Ukraine's critical infrastructure on a large scale, as electric power and Internet services remain up and running in many parts of Ukraine, including some that have been bombed or shelled. Tactically, Russian military operations have used a variety of traditional battlefield tactics, techniques, and procedures, but with cyber operations playing a significantly lesser role.

This article explores the use of offensive cyber operations in the Russia-Ukraine conflict as they have been seen and discussed in the public domain.

On the Value of Offensive Cyber Operations

Analysts often distinguish between coercive and warfighting uses of military force. Coercive uses of or threats to use force seek to influence an adversary's decisions, whereas warfighting uses of force seek to degrade an adversary's military power or effectiveness.

The international relations literature persuasively establishes that successful coercion is not simply a matter of a more militarily powerful party asserting dominance over a less powerful one—coercion is a more complex endeavor and success is less certain. Vast nuclear superiority is widely believed to have coerced Japan's surrender in World War II and the Soviet Union to back down during the Cuban Missile Crisis. However, the record on non-nuclear coercion is much more mixed. As Byman and Waxman put it, "[w]hile the US military arsenal may be extremely precise in a technological sense, the ability to finely tune the political effects its use has on an adversary's population, elite, or key regime decision makers remains largely beyond U.S. planners."[20]

How, if at all, does the capability to launch powerful cyberattacks change these conclusions? On the first, how, if at all, does the ability to exercise significant offensive cyber capabilities give nations greater coercive power against their adversaries? On the second, how, if at all, does the use of significant offensive cyber capabilities enhance the warfighting effectiveness of a nation's armed forces?

Note –
Physically-Mediated Cyberattacks on Ukraine

On May 13, 2022, the State Service of Special Communication and Information Protection of Ukraine published a notice alleging that "Russia's special services" had physically targeted Ukrainian internet service providers (ISPs).[18] Apparently, the Russians military physically invaded the offices of Stratus, a Ukrainian internet service provider located in Kherson, and at the point of a gun, ordered the staff in the office to alter the availability of websites that users of the service would normally be able to access.

Such outcomes could, of course, be caused through various cyberattacks carried across the internet. But attacks that compromise cyber functionality through the use of or the threat of physical force are an understudied phenomenon.

Two points are particularly relevant here. First, insider attacks are a well-known problem in cybersecurity. Trusted (authorized) insiders can be "turned" to take actions for which they have the proper technical authorization but for purposes that are contrary to the rationale for granting those authorizations in the first place.

Second, the physical facilities of ISPs have also been known to be vulnerable, as exemplified by cuts in fiber-optic cables resulting in denials of service to customers depending on those cables. That is, the physical security of cyber infrastructure has always been an important, if often neglected, aspect of cybersecurity.

While a demand for an ISP located in a region under Russian military occupation to conform to Moscow's pressure regarding Internet connectivity is not surprising, one can also imagine similar activities directed against ISPs located in other regions whose governance is contested. Physical violence against cyber personnel in lawless environments as an element of cyberattack is another dimension of cyber conflict, and its importance has been neglected for way too long. But we do not even have a category in the cyber conflict lexicon to address its nature or significance.[19]

As an important preliminary point, offensive cyber capabilities do provide nations with additional instruments of covert action (e.g., sabotage, espionage, and political subversion).[21] Through actions taken in cyberspace, nations can cause physical damage to important facilities as demonstrated in the outcome of cyberattacks against Iranian uranium centrifuges and steel mills in 2010 and 2022, respectively.[22] They can also steal confidential information of high economic or intelligence value,[23] sometimes in sufficient quantity to be of strategic significance.[24] Finally, they can interfere in democratic political processes, such as elections.[25] Although sabotage, espionage, and political subversion are distinctly hostile acts that seek to weaken adversaries, they are neither acts of coercion (they are not undertaken in an attempt to seek concessions from adversaries) nor acts of warfighting. Several analysts believe that a relative insignificance of cyberattacks in the Russian-Ukraine conflict validates this view.[26]

Not all analysts share this view, however. Arguing before February 24 in favor of the proposition that offensive cyber capabilities do increase coercive power, William Courtney and Peter A. Wilson wrote in *The Hill* that a Russian invasion would "likely employ massive cyber and electronic warfare tools and long-range PGMs . . . to create 'shock and awe,' [and] causing Ukraine's defenses or will to fight to collapse."[27] Jason Healey of Columbia University said that "a Russian cyber offensive . . . might have far more impact on the battlefield, more coercive power, more lethal and widespread effect than many doubters would expect."[28]

As for warfighting potential, the U.S. Department of Defense (DoD) asserts a rather broad utility for offensive cyber operations. For example, Joint Publication 3-12 characterizes cyberattacks as a form of fires,[29] similar in principle to artillery or machine-gun fire, that degrades, disrupts, destroys, or manipulates adversary information or information systems. DoD doctrine also acknowledges the value of cyber operations for exploitation, including military intelligence activities, maneuver, information collection, and other enabling actions required to prepare for future military operations.[30]

THE STRATEGIC PERSPECTIVE

As noted earlier, Russian cyber operations against Ukraine have apparently had little coercive effect on Ukraine. This section explores possible reasons for this outcome.

First, prophylactic defensive measures by Ukrainian and Western cyber experts may have borne significant fruit in hardening many Ukrainian critical infrastructure systems. Since 2014, Ukraine has served as a kind of cyber test range for Russian cyber attackers, but the US, the European Union, and NATO member states have provided cybersecurity assistance to help Ukraine prepare for future attacks. For example, the U.S. Agency for International Development announced in 2020 that it was investing $38 million in Ukrainian cybersecurity over four years.[31] On March 10, 2022, General Paul Nakasone, Commander of U.S. Cyber Command (USCYBERCOM), testified to the Senate Intelligence Committee that "we've worked very, very hard with Ukraine over the past several years. . . We had 'hunt forward' teams from U.S. Cyber Command in Kyiv. We worked very, very closely with a series of partners at NSA and the private sector to be able to provide that information."[32] The US has also helped to broker a number of public-private partnerships between Ukraine and Western information technology companies such as Microsoft and Google. These companies identified and blocked Russian cyber threats against Ukraine in near-real-time as they emerged,[33] and their familiarity with and instrumentation of Ukrainian networks enabled them to act more rapidly than government agencies.

Second, Ukraine or Western military or intelligence organizations may themselves have been conducting offensive cyber operations against Russian hackers to disrupt cyberattacks against Ukraine. Information about any such operations would be highly classified, but on March 10, 2022, Anne Neuberger, Deputy National Security Advisor to the President for Cyber & Emerging Technology, described a three-part strategy for responding to Russian cyberattacks against Ukraine, one of which was to "make it harder for attackers to conduct disruptive operations, whether that is disrupting [their] infrastructure and more sensitive operations that I won't get into here."[34] A precedent for such activity may have been the reported disruption of the Internet Research Agency, a Russian troll farm, by USCYBERCOM[35]—according to *The Washington Post*, offensive actions by USCYBERCOM blocked Internet access for the IRA on election day, 2018. Similar actions could have disrupted the operations of Russian hacker groups targeting Ukraine.

Nor are Western government agencies the only parties capable of conducting offensive cyber operations against Russia. A variety of news reports indicates that non-government hackers have acted against Russian information systems, including actions to slow the transport of Russian troops and equipment by putting the trains into a manual control mode,[36] breaching Russian databases and hacking Russian media and government websites,[37] and releasing personal information on Russian soldiers who operated in Bucha, as well as Russian intelligence agents in the Federal Security Service (FSB).[38] On balance, such activities force Russian cyber forces to expend considerable time and effort on countermeasures,[39] leaving them with fewer resources to go on the offensive themselves.

Third, the apparent paucity of Russian cyberattacks may also reflect their omission from the Russian planning process for the invasion. Integrating offensive cyber capabilities into an overall military operational plan is relatively new, compared to more traditional military capabilities such as armor and artillery. Russian military leaders seemed caught off-guard when relatively simple logistical problems slowed the invasion to a snail's pace, and there is no reason to conclude that planning deficiencies were limited to the logistical aspects of ground combat—Russian military planners may simply have neglected or consciously chosen to omit Russian offensive cyber capabilities in their invasion plan. Supporting this possibility, Ciaran Martin, former head of the UK National Cyber-Security Centre, noted that "if . . . Putin withheld knowledge of his invasion plans from large sections of the Russian military and intelligence bureaucracy, then they wouldn't have had time to prepare those attacks, and you can't just conjure up a powerful cyberattack overnight."[40]

Fourth, Russia may want to keep its cyber powder dry for use against the West if and when necessary. Former CISA director Chris Krebs wrote on March 20, 2022, that "as political and economic conditions deteriorate, the red lines and escalation judgments that kept Moscow's most potent cyber capabilities in check may adjust. Western sanctions and lethal aid support to Ukraine may prompt Russian hackers to lash out against the west."[41] Around the same time, Senate Intelligence Committee Chair Mark Warner told *Politico* that "we have not seen their A-game tools."[42] In this view, the Russians may believe that the likelihood of successfully conducting specific offensive cyber operations diminishes the more they are used, and are saving their most potent weapons for later use.

Lastly, previous cyberattacks targeting Ukrainian critical infrastructure have been conducted at a level considerably below a "whole-of-country" effort. These cyberattacks constituted proofs of principle of Russian cyber capabilities, at least against the Ukrainian cyber defenses of the time, but many in the West extrapolated from such demonstrations a capability to attack all Ukrainian critical infrastructure more or less simultaneously in an all-out prelude to the ground invasion. Such extrapolations rely on an assumption that resource constraints did not exist for Russian cyber attackers, and perhaps in reality resource constraints have prevented a significant scaling-up of Russian cyberattacks. Moreover, to the extent that Russian offensive

cyber operations would be conducted wirelessly, cyber operations deep in the heart of Ukraine would likely be more challenging to coordinate than those that were mostly contained on the Russia-Ukraine border, as many such previous Russian operations had been.[43]

THE TACTICAL PERSPECTIVE

The intense kinetic attack on Ukraine has caused extensive damage to Ukrainian infrastructure, which may well have reduced the need to use cyberattacks to target infrastructure as part of the invasion. Dmitri Alperovitch, founder of the cybersecurity company CrowdStrike, noted that "cyber is a fantastic tool for gray-zone conflict, that area between peace and war, where you are trying to hit back at the other party, but you don't want to escalate this to an actual kinetic conflict... [but] once conflict actually begins, once bombs are flying, cyber becomes much less useful."[44] Christopher Painter, former State Department cybersecurity coordinator, observed that "physical invasion trumps cyber. . . You don't need cyber as much when you have tanks and planes on the ground and men on the ground, so maybe cyber ... maybe it isn't the perfect weapon."[45] Ciaran Martin, former head of the United Kingdom's National Cyber Security Center, has suggested that Russia may have wished to preserve Ukrainian infrastructure for use during the invasion,[46] especially for communications assets such as cell phone networks.[47] (Note that these explanations seem somewhat contradictory—the first saying that Russians refrained from cyberattacks because kinetic weapons are pulverizing the infrastructure and the second saying that it is because the Russians wanted to maintain the infrastructure in operable condition for their own use. Still, both reasons could be operative at the same time.)

The remainder of this section discusses some of the important reasons that the role of cyberattack in most combined-arms operational plans is inherently circumscribed. A key first step in directing fires is to identify suitable targets. Many kinetic targets are well-known and well-characterized—e.g., military bases, headquarters buildings, ammunition and fuel storage facilities, and telecommunications facilities. Accessing these targets can be planned as routes through three-dimensional physical space. By contrast, many targets in cyberspace appear and disappear from the Internet with the flick of a switch, to say nothing of an access path to them. Even worse, targets that minimize use of networked information technology are less vulnerable to offensive cyber operations. Note that this statement is not synonymous with the use of advanced technology. For example, a Javelin anti-tank missile makes extensive use of digital electronics, but it is not connected to other systems (i.e., it is not networked). Thus, a cyber operation to disable Javelin missiles must be conducted on each individual missile—a daunting task on a fast-moving battlefield.[48]

Matching weapons to targets is an important second step. Compared to kinetic weapons, the effectiveness of a cyber weapon depends heavily on the target's characteristics. Any ship hit by a torpedo with a sufficiently large warhead will be damaged, whether the ship is made of wood or steel. Anything within the crater of a nuclear weapon will be destroyed, regardless of how it

was built. A few physical parameters (e.g., target hardness, yield of weapon, distance between point of weapon impact and the target) mostly determine the damage suffered in a kinetic attack. The nature of target-weapon interaction with kinetic weapons can usually be estimated based on physics experimentation and calculation. Most importantly, a sufficiently small but non-zero change in the properties of the target or the weapon generally will result in a small change in the damage inflicted by the weapon.

This is not true for target-weapon interactions in cyberspace, because the alteration of a cyber target by one bit, which is the smallest change possible in a cyber target's characteristics, can completely change the response of the target to the weapon. For example, it may be a one-bit difference in configuration that instructs a targeted system to accept or not to accept data from the Internet. Set one way, a bit can enable an adversary to gain access to the target through the Internet using a particular technique. Set the other way, the use of that technique can be entirely prevented, and thus a cyberattack based on that technique will have no effect at all on the targeted system. In cyberspace, physics and continuous mathematics provide no assistance in calculating or estimating expected effects.

Extreme dependency on small details as to target characteristics has several deleterious consequences that increase the difficulty of making accurate predictions about the outcomes of an offensive cyber operation. For example, in contrast to kinetic weapons, the weapons and capabilities of offensive cyber operations are often customized in detail to the specific target(s) against which these operations may be directed, particularly when precision of attack is needed (for example, to minimize collateral damage). Yet customization generally is time-intensive and technically demanding.[49] Put differently, "off the shelf" weapons and capabilities to support offensive cyber operations are far less available than is the case with their kinetic counterparts.

Intelligence information on target characteristics must also be precise, high-volume, high-quality, current, and available at the time of the weapon's use. For example, key intelligence information may include whether a certain patch has been installed in the target's operating system. Unless the targets of interest have been extensively probed ("prepared") in advance, such detailed information is generally unavailable on a timely basis in a highly dynamic environment, especially in battlefield environments in which individual platforms are online and offline at unpredictable intervals.

Assuming that targets have been identified and offensive capabilities programmed against them, a subsequent step is to conduct the cyberattack. However, two timelines must be compatible if the cyberattack is to be useful. The first is how long it takes for a cyberattack to realize its effects on its target. The second is driven by the overall operational plan, which will often involve other military operations conducted on land, in the air or space, or at sea.

One of the most critical dimensions of an operational plan is proper synchronization of the various activities in the plan, without which the effectiveness of the plan can be significantly

diminished. For example, adversary surface-to-air missile sites and radars need to be destroyed or disabled before friendly penetrating aircraft come into range—suppression of enemy air defenses (SEAD) after that point will do much less to enhance bomber penetrativity.

Success rates are quite high for cyberattackers who have the luxury of unlimited time to penetrate a target's cyber defenses, yet no reasonable operational plan allows for unlimited time frames. In addition, the time needed to penetrate adversary defenses is highly variable—it may take a few minutes or many days, depending on the attacker's luck of the draw. While no defense, no matter how strong, can withstand a concerted cyberattack indefinitely, robust defenses can prolong the time it takes for an adversary to succeed. Such delays can upend the synchronization of an operational plan and thereby significantly diminish the impact of cyberattacks.

To reduce time delays and make attack timelines more predictable, would-be attackers often try to prepare a cyber target well before the actual attack, for example, by surreptitiously installing a "back door" that gives the attacker access at a later time. Such access can be used to download a customized attack payload that accounts for new intelligence information becoming available. Advance preparation facilitates prompt access that circumvents the target's cyber defenses, but many targets are not susceptible to being prepared in advance.

Lastly, in contrast to kinetic attacks, the state of the art in assessing damage caused by cyberattacks is still primitive. Damage caused by a cyberattack is usually invisible to the human eye. Returning to the SEAD scenario—if the intent of the cyberattack is to turn off the power to a specific radar installation in the nation's air defense network at a specific time, it will be difficult to distinguish between a successful attack and a smart and wily defender who has detected the attack, shut the power down, and can turn it back on at a moment's notice. By contrast, a radar destroyed by an anti-radiation missile leaves debris scattered about and a smoking hole in the ground, visually confirming a successful attack. Commanders need to know that a SEAD attack was successful, and attacking with an anti-radiation missile is more likely to yield a high-confidence answer than the use of a cyberattack. In integrating cyberattack into combined arms operational planning, commanders must therefore expect greater uncertainty with cyberattacks than with their physical world counterparts, which in turn may cause more reliance on the latter depending upon the mission.

CONCLUSION

The Cyber Peace Institute's timeline of cyberattacks on Ukraine confirmed an uptick in the weeks before the ground invasion began,[50] but these attacks were more or less consistent in intensity and significance to other attacks that Ukraine had experienced over the past several years. By contrast, in the weeks and months before the invasion, Russia deployed unprecedented numbers of troops to Russian-Ukrainian borders. These deployments understandably took

center stage in the Ukrainian consciousness, and these troops—rather than the cyberattacks—were widely viewed as the primary element of an attempt to force Ukraine to accede to Russian political demands, such as a change in the Ukrainian constitution to forbid NATO membership permanently. In any event, given Ukraine did not accede to Russian demands, it is fair to say that neither Russian cyber operations nor troops were successfully brandished to achieve a coercive effect on Ukraine.

What about warfighting? How and to what extent, if any, have Russian offensive cyber capabilities improved Russia's ability to degrade Ukrainian military power or effectiveness? There have been no reports of cyberattacks against Ukrainian weapons systems or military command and control systems per se. As suggested above, cyberattacks are less effective against targets in the category of "absolutely, positively must be destroyed or disabled with high confidence and certainty or on a certain timetable."

On the other hand, cyberattacks can be more useful when directed against a target set consisting of many entities, only some of which need to be destroyed or disabled to have a significant effect. (This attack scenario would be analogous to the Nigerian prince seeking suckers who will send him money and sending out millions of emails, knowing that he will make money even if only a very small fraction of recipients responds positively. In this case, the prince does not particularly care who responds, only that some do.) Moreover, cyberattackers who are indifferent to any external timetable can take as much time as needed to obtain results.

The planning and operational coordination of cyberattacks that satisfy the "some out of many" condition above is also much simpler. A relatively simple statement of intent to the cyberattackers likely suffices for command and control—"go forth and damage Ukrainian institutions that provide government, military, and economic functions, that inform the Ukrainian public, or that constitute Ukrainian critical infrastructure."[51] Such cyber operations need not be timed carefully to synchronize with other operations, yet a large number of cyber operations occurring in the same general time frame with a large number of kinetic operations will often result in some of each happening contemporaneously. Thus, it may appear as though cyber and kinetic operations were deliberately synchronized. Many of the cyberattacks conducted against Ukrainian infrastructure in the days immediately after February 24 appear to be of this nature.

It is also noteworthy that the synchronization of cyberattacks with a larger operational plan is not needed; such attacks can be conducted by parties other than Russian military cyber operators. Russian cybercriminal groups are quite capable of conducting such attacks on their own, and should they do so their activities would be largely indistinguishable from those of military cyber operators, at least initially.

Finally, in trying to understand the significance of Russian offensive cyber operations against Ukraine, it is important to keep two points in mind. First, many possible reasons have been offered as explanations for the paucity of Russian offensive cyber operations against Ukraine; others no doubt will be posited in the future. It is almost certainly true that there are multiple reasons for this surprising outcome. Ground truth on the "real" story will be elusive, pending debriefings with senior Russian commanders and other decision-makers (a prospect that does not appear probable any time in the near future).

Second, as of this writing, the war is still going on, it still appears to be indefinite in duration—nowhere near conclusion, and its outcome remains in doubt. If the ground invasion continues to stall, Russia may yet turn to large-scale cyberattacks,[52] either on Ukraine or the West or both, to put pressure on Ukraine for concessions or on the West to cease or cut back on its military support for Ukraine. Such attacks would depend on high-level decisions and resource availability (i.e., tools, personnel, and knowledge/intelligence). At this point, however, it is simply a fact that Western intelligence sources lack insight into what senior Russian decision-makers will choose to do in the future. Thus, conclusions regarding the importance of cyber operations to the conduct of the Russian-Ukraine war are preliminary at best, and generalizations about the strategic utility of offensive cyber operations for coercion are almost certainly premature.

ACKNOWLEDGMENTS

I gratefully acknowledge the assistance of Thomas Berson, Gil Baram, Joseph Nye, Brandon Williams, and two reviewers for commentary on earlier drafts of this paper. Errors and other inadvertent misinformation are my responsibility alone.

NOTES

1. 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. "Will war in Ukraine lead to a wider cyber-conflict?" *The Economist*, February 23, 2022, www.economist.com/europe/2022/02/23/will-war-in-ukraine-lead-to-a-wider-cyber-conflict.
3. Nadiya Kostyuk and Erik Gartzke, "Cyberattacks have yet to play a significant role in Russia's battlefield operations in Ukraine – cyberwarfare experts explain the likely reasons," *The Conversation*, April 4, 2022, theconversation.com/cyberattacks-have-yet-to-play-a-significant-role-in-russias-battlefield-operations-in-ukraine-cyberwarfare-experts-explain-the-likely-reasons-178604.
4. 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, warontherocks.com/2022/02/there-is-no-cyber-shock-and-awe-plausible-threats-in-the-ukrainian-conflict/.
5. Andry Greenberg, "Russia's Sandworm Hackers Attempted a Third Blackout in Ukraine," *Wired,* April 12, 2022, www.wired.com/story/sandworm-russia-ukraine-blackout-gru/.
6. Patrick Howell O'Neill, "Russian hackers tried to bring down Ukraine's power grid to help the invasion," *MIT Technology Review*, April 12, 2022, www.technologyreview.com/2022/04/12/1049586/russian-hackers-tried-to-bring-down-ukraines-power-grid-to-help-the-invasion/.
7. Sean Lyngaas, "US Satellite operator says persistent cyberattack at beginning of Ukraine war affected tens of thousands of customers," *CNN*, March 30, 2022, www.cnn.com/2022/03/30/politics/ukraine-cyberattack-viasat-satellite/index.html.
8. Kim Zetter, "Viasat Hack 'Did Not' Have Huge Impact on Ukrainian Military Communications, Official Says," Substack newsletter, *Zero Day* (blog), September 26, 2022, https://zetter.substack.com/p/viasat-hack-did-not-have-huge-impact.
9. Kyle Fendorf and Jessie Miller, "Tracking Cyber Operations and Actors," Council on Foreign Relations, March 24, 2022, www.cfr.org/blog/tracking-cyber-operations-and-actors-russia-ukraine-war.
10. Presentation by Rob Joyce, director of cybersecurity at NSA, "State of the Hack: NSA's Perspective," *RSA Conference,* San Francisco, June 7, 2022.
11. Dan Goodin, "Mystery solved in destructive attack," *Ars Technica*, March 31, 2022, arstechnica.com/information-technology/2022/03/mystery-solved-in-destructive-attack-that-knocked-out-10k-viasat-modems/; "Ukraine: Timeline of Cyberattacks on critical infrastructure and civilian objects," Cyber Peace Institute, May 12, 2022, cyberpeaceinstitute.org/ukraine-timeline-of-cyberattacks/.
12. "Ukraine: Timeline of Cyberattacks."
13. Valerie Insinna, "SpaceX beating Russian jamming attack was 'eyewatering': DoD official," *Breaking Defense*, April 20, 2022, breakingdefense.com/2022/04/spacex-beating-russian-jamming-attack-was-eyewatering-dod-official/.
14. "Ukraine: Timeline of Cyberattacks."
15. Charlie Osborne, "Ukraine destroys five bot farms that were spreading 'panic' among citizens," *ZDnet,* March 29, 2022, www.zdnet.com/article/ukraine-takes-out-five-bot-farms-spreading-panic-among-citizens/.
16. David Cattler and Daniel Black, "The Myth of the Missing Cyberwar: Russia's Hacking Succeeded in Ukraine—And Poses a Threat Elsewhere, Too," *Foreign Affairs,* April 6, 2022, www.foreignaffairs.com/articles/ukraine/2022-04-06/myth-missing-cyberwar.
17. "Special Report: Ukraine. An overview of Russia's cyberattack activity in Ukraine." *Microsoft Digital Security Unit*, April 27, 2022, query.prod.cms.rt.microsoft.com/cms/api/am/binary/RE4Vwwd.
18. State Service of Special Communications and Information Protection of Ukraine, May 5, 2022, https://cip.gov.ua/en/news/okupanti-shantazhem-i-pogrozami-zmushuyut-ukrayinskikh-provaideriv-pidklyuchatisya-do-rosiiskikh-merezh.
19. Herbert Lin, "The Emergence of Physically Mediated Cyberattacks?," *Lawfare*, May 21, 2022, https://www.lawfareblog.com/emergence-physically-mediated-cyberattacks.
20. Daniel Byman and Matthew Waxman, *Dynamics of Coercion: American Foreign Policy and the Limits of American Military Might* (New York: Cambridge University Press, 2002), 236.
21. Thomas Rid, "What Would a Real Cyberwar Look Like?" *Slate*, September 15, 2013, slate.com/technology/2013/09/cyberwar-and-cyberattacks-its-really-espionage-subversion-or-sabotage.html; Joshua Rovner, "Cyber War as an Intelligence Contest," *War on the Rocks,* September 16, 2019, warontherocks.com/2019/09/cyber-war-as-an-intelligence-contest/.

NOTES

22. On the first, see Kim Zetter, "An Unprecedented Look at Stuxnet, the World's First Digital Weapon," *WIRED,* November 3, 2014, https://www.wired.com/2014/11/countdown-to-zero-day-stuxnet/. On the second, see Isabel Debre, "Large Cyberattack on Iranian Industrial Sector Targets Three Steel Plants," *Times of Israel*, June 28, 2022, https://www.timesofisrael.com/large-cyberattack-on-iranian-industrial-sector-targets-three-steel-plants/.
23. On economic value, see "The Economic Impact of Cybercrime and Cyber Espionage," Center for Strategic and International Studies, July 2013, http://csis-website-prod.s3.amazonaws.com/s3fs-public/legacy_files/files/publication/60396rpt_cybercrime-cost_0713_ph4_0.pdf; on intelligence value, see National Counterintelligence and Security Center, Cyber Aware Case Study-Office of Personnel Management, Office of the Director of National Intelligence, https://www.dni.gov/ncsc/e-Learning_CyberAware/pdf/Cyber_Aware_CaseStudy_OPM.pdf; Michael Adams, "Why the OPM Hack Is Far Worse Than You Imagine," *Lawfare*, March 11, 2016, https://www.lawfareblog.com/why-opm-hack-far-worse-you-imagine.
24. Josh Rogin, "NSA Chief: Cybercrime constitutes the 'greatest transfer of wealth in history'," *Foreign Policy*, July 9, 2012, https://foreignpolicy.com/2012/07/09/nsa-chief-cybercrime-constitutes-the-greatest-transfer-of-wealth-in-history/.
25. See, for example, Robert S. Mueller, III, "Report On Yhe Investigation Into Russian Interference In The 2016 Presidential Election," U.S. Department of Justice, March 2019, Volumes I and II (https://www.justice.gov/archives/sco/file/1373816/download.
26. See, for example, John Popham, "Russia's Failure in Cyberspace," Georgia Institute of Technology, March 10, 2022, www.cc.gatech.edu/news/russias-failure-cyberspace.
27. William Courtney and Peter A. Wilson, "Expect 'shock and awe' if Russia invades Ukraine," *The Hill,* December 8, 2021, https://thehill.com/opinion/international/584805-expect-shock-and-awe-if-russia-invades-ukraine.
28. Joseph Marks, "Here's what cyber pros are watching in the Ukraine conflict," *The Washington Post*, February 24, 2022, https://www.washingtonpost.com/politics/2022/02/24/heres-what-cyber-pros-are-watching-ukraine-conflict/.
29. Joint Publication 3-12, *Cyberspace Operations,* Joint Chiefs of Staff, Department of Defense, June 8, 2018, II-7, https://www.jcs.mil/Portals/36/Documents/Doctrine/pubs/jp3_12.pdf; Fires refer to the use of weapons systems to create specific effects on a target; See Joint Publication 3-0, *Joint Operations*, Joint Chiefs of Staff, Department of Defense, January 17, 2017, Incorporating Change 1 October 22, 2018, , irp.fas.org/doddir/dod/jp3_0.pdf, III-30.
30. Joint Publication 3-12, *Cyberspace Operations,* Joint Chiefs of Staff, Department of Defense, June 8, 2018, II-6, https://www.jcs.mil/Portals/36/Documents/Doctrine/pubs/jp3_12.pdf.
31. Maggie Miller, "Despite years of preparation, Ukraine's electric grid still an easy target for Russian hackers," *Politico,* February 19, 2022, www.politico.com/news/2022/02/19/despite-years-of-preparation-ukraines-electric-grid-still-far-from-ready-for-russian-hackers-00010373.
32. United States Senate Select Committee on Intelligence, "Hearing on Worldwide Threats," *Committee Hearing Channels,* March 10, 2022, (02:20:41), www.intelligence.senate.gov/hearings/open-hearing-worldwide-threats-2.
33. David E. Sanger, Julian E. Barnes, and Kate Conger, "As Tanks Rolled Into Ukraine, So Did Malware. Then Microsoft Entered the War," *The New York Times*, February 28, 2022, www.nytimes.com/2022/02/28/us/politics/ukraine-russia-microsoft.html.
34. Kara Swisher, "Are We Ready for Putin's Cyber War? I Asked One of Biden's Top Cybersecurity Officials," *Sway, The New York Times*, guest speaker Anne Neuberger, March 10, 2022, www.nytimes.com/2022/03/10/opinion/sway-kara-swisher-anne-neuberger.html.
35. Ellen Nakashima, "U.S. Cyber Command operation disrupted Internet access of Russian troll factory on day of 2018 midterms," *The Washington Post,* February 27, 2019, www-washingtonpost-com/world/national-security/us-cyber-command-operation-disrupted-internet-access-of-russian-troll-factory-on-day-of-2018-midterms/2019/02/26/1827fc9e-36d6-11e9-af5b-b51b7ff322e9_story.html.
36. Ryan Gallagher and Bloomberg, "Hackers in Belarus claim to have disrupted trains to 'slow down the transfer' of Russian troops into Ukraine," *Fortune*, February 27, 2022, fortune.com/2022/02/27/belarus-hackers-disrupt-trains-russia-invasion-ukraine-cyber-partisans/.
37. Monica Buchanan Pitrelli, "Anonymous declared a 'cyber war' against Russia, Here are the results" *CNBC,* March 16, 2022, www.cnbc.com/2022/03/16/what-has-anonymous-done-to-russia-here-are-the-results-.html.
38. Kate Conger and David E. Sanger, "Hackers Claim to Target Russian Institutions in Barrage of Cyberattacks and Leaks," *The New York Times*, April 22, 2022, www.nytimes.com/2022/04/22/us/politics/hackers-russia-cyberattacks.html.

NOTES

39. Danielle Kurtzleben, "Volunteer hackers form 'IT Army' to help Ukraine right Russia," *All Things Considered*, NPR, guest speaker Dina Temple-Raston, March 27, 2022, www.npr.org/2022/03/27/1089072560/volunteer-hackers-form-it-army-to-help-ukraine-fight-russia.
40. Maggie Miller, "The world holds its breath for Putin's cyberwar." *Politico*, March 23, 2022, www.politico.com/news/2022/03/23/russia-ukraine-cyberwar-putin-00019440.
41. Chris Krebs, "The cyber warfare predicted in Ukraine may be yet to come," *Financial Times,* March 20, 2022, www-ft-com/content/2938a3cd-1825-4013-8219-4ee6342e20ca.
42. Miller, "The world holds its breath."
43. Insinna, "SpaceX beating Russian jamming attack was 'eyewatering'."
44. Ibid.
45. Ibid.
46. "Cyber-attacks on Ukraine are conspicuous by their absence," *The Economist*, March 1, 2022, www.economist.com/europe/2022/03/01/cyber-attacks-on-ukraine-are-conspicuous-by-their-absence.
47. As one example, Era is a Russian communications system that is designed to provide secure, encrypted communications for personnel on the ground. However, its use requires the presence of an existing 3G or 4G wireless communications network. It is thus unfortunate, from the Russian point of view, that the Russian ground assault destroyed a substantial number of Ukrainian 3G/4G towers, thus forcing Russian soldiers to use less secure methods of communication (Rob Waugh, "'Idiots': Russian military phone calls hacked after own soldiers destroy 3G towers," *yahoo!news*, March 8, 2022, news.yahoo.com/russian-military-being-hacked-after-its-own-soldiers-destroy-3-g-internet-towers-104303881.html.)
48. In principle, a supply chain attack on the digital electronics used in such missiles could be part of an effort to disable them when put into use, but triggering such an attack without real-time access to the missiles would be quite difficult.
49. Steven M. Bellovin, Susan Landau, and Herbert S. Lin, "Limiting the Undesired Impact of Cyber Weapons: Technical Requirements and Policy Implications," *Journal of Cybersecurity* 3(1):59-68, March 1, 2017, https://academic.oup.com/cybersecurity/article/3/1/59/3097802.
50. "Ukraine: Timeline of Cyberattacks."
51. "Special Report: Ukraine. An overview of Russia's cyberattack activity in Ukraine." *Microsoft Digital Security Unit,* April 27, 2022, query.prod.cms.rt.microsoft.com/cms/api/am/binary/RE4Vwwd.
52. For example, on April 20, 2022, the cybersecurity authorities of the Five Eyes warned private sector organizations that Russia's invasion of Ukraine could expose organizations both within and beyond the region to increased malicious cyber activity, https://www.cisa.gov/uscert/ncas/alerts/aa22-110a.