doi:10.1017/aju.2022.20

SYMPOSIUM ON UKRAINE AND THE INTERNATIONAL ORDER

UKRAINE, CYBERATTACKS, AND THE LESSONS FOR INTERNATIONAL LAW

*Kristen E. Eichensehr**

Russia's invasion of Ukraine has put to the test theories about how cyberattacks fit into conventional war. Contrary to many expectations, cyber operations appear to have played only a limited role in the initial stages of the invasion, prompting competing theories and rampant speculation about why. Although written while the conflict continues, this essay considers how either of two broad explanations for the limited role of cyberattacks to date—that Russia's attempted cyberattacks were thwarted or that Russia chose not to deploy them widely—challenges conventional wisdom about cybersecurity. The essay concludes by suggesting that one lesson international lawyers should draw from the current conflict is the urgent need to clarify and enforce international rules not just for the rare high-end destructive or widely disruptive cyber operations, but also for lower-level operations that have proven more consistently problematic, both in Ukraine and elsewhere. Clarifying such rules could help to manage escalation risk now and in the future, even if such rules—like the most venerable international law prohibitions that Russia's invasion has violated—do not necessarily restrain behavior directly.

The Limited Role of Cyber Operations So Far

In the build-up to Russia's invasion, experts raised concerns about Russian cyberattacks on Ukraine and potential spillover into other countries. There is precedent for both. In 2015 and 2016, Russia launched cyber operations that knocked out power in Ukraine, and in 2017, Russia used Ukrainian accounting software to launch destructive malware known as NotPetya that although disguised as ransomware, actually "irreversibly encrypted" files, rendering ransom payments "futile."[1] NotPetya spread worldwide, causing $10 billion in damage.[2]

Given this history and years of speculation about what war by a cyber power would look like, expectations were high that cyber operations would play a major role in the initial invasion. Instead, their role appears to have been relatively limited, prompting surprise among many who follow Russia's cyber operations. Senate Intelligence Committee Chairman Mark Warner, for example, declared that he was "'amazed that [the Russians] have not really launched the level of maliciousness that their cyber arsenal includes.'"[3]

The known cybersecurity incidents in the lead up to and weeks immediately following the invasion have been relatively modest in effect.[4] For example, in mid-February, a distributed denial of service (DDOS) attack by the

* *Martha Lubin Karsh and Bruce A. Karsh Bicentennial Professor, University of Virginia School of Law, United States.* *For helpful comments, thanks to Gary Corn, Josh Goland, Jack Goldsmith, Duncan Hollis, Dev Ranjan, and Richard Re.*

[1] Andy Greenberg, *The Untold Story of NotPetya, the Most Devastating Cyberattack in History*, WIRED (Aug. 22, 2018).

[2] *Id.*

[3] Ines Kagubare, *Intel Chair "Amazed" Russia Hasn't Launched Full-Scale Cyberwarfare*, HILL (Mar. 14, 2022).

[4] For a helpful tracker, see CyberPeace Institute, *Ukraine: Timeline of Cyberattacks on Critical Infrastructure and Civilian Objects*.

Russian military briefly disrupted access to the websites of several government departments and the two largest Ukrainian banks,[5] and cyber operations have intermittently disrupted some internet services.[6] Researchers have also discovered several types of wiper malware, which destroys or corrupts data, on Ukrainian systems both before and after the invasion, though the malware appears to have caused limited damage to date.[7]

The most significant cybersecurity incident disclosed so far is also the one most like the sort of cyberattacks expected to accompany the invasion. As the invasion commenced on February 24, 2022, the Russian government launched a cyberattack targeting broadband internet services provided by Viasat, a company that is a U.S. defense contractor and that has contracts with Ukraine's military and police.[8] A Ukrainian official later told reporters that the incident "resulted in a 'huge loss in communications in the very beginning of the war.'"[9] The intrusion disrupted satellite internet access across Europe, including in Poland and France, and in Germany, thousands of wind turbines remained offline a month after the incident.[10] Disruptive as this incident has been, it is notable as apparently the only major successful cyberattack of the kind that many expected to blanket Ukraine at the outset of the invasion.

Why Haven't Cyberattacks Played a Bigger Role?

In the fog of war, cyber operations may be the foggiest component of all—at least to those outside governments and sophisticated companies. But uncertainty has not stopped speculation. The *Washington Post* recently catalogued no fewer than eleven possible explanations for the limited successful cyber operations accompanying Russia's invasion.[11] In time, what actually happened (or did not) on the cyber front will become clearer, and Ukraine seems destined to become a watershed case study for whichever explanations turn out to be correct. In the meantime, the remainder of this essay attempts to systematize some of the theories about muted cyber operations in order to shed light on what international lawyers and policy makers might ultimately learn from the role of cyber operations in the Russian invasion.

At the broadest level of generality, there are two categories of possible explanations for the limited cyber effects in the early weeks of the conflict: (1) attempted or planned cyberattacks failed; or (2) Russia chose not to launch widespread cyberattacks. Both options challenge conventional wisdom and suggest lessons going forward.

Turning to the first option, if Russia planned or attempted cyberattacks, but failed to achieve significant destruction or disruption, that might suggest that cyber defenses succeeded. A story in which Russian cyber operations proved less effective than expected would fit with the broader picture of the invasion, where Russia failed to achieve its initial objectives with conventional military forces, apparently due to poor planning and underestimating Ukrainian defenses.[12]

[5] Steve Holland & James Pearson, *US, UK: Russia Responsible for Cyberattack Against Ukrainian Banks*, Reuters (Feb. 18, 2022).

[6] Christopher Bing & Raphael Satter, *Ukrainian Telecom Company's Internet Service Disrupted by "Powerful" Cyberattack*, Reuters (Mar. 28, 2022).

[7] *See, e.g.*, Sergiu Gatlan, *New CaddyWiper Data Wiping Malware Hits Ukrainian Networks*, Bleeping Computer (Mar. 14, 2022).

[8] James Pearson, Raphael Satter, Christopher Bing & Joel Schectman, *Exclusive: U.S. Spy Agency Probes Sabotage of Satellite Internet During Russian Invasion, Sources Say*, Reuters (Mar. 11, 2022); David E. Sanger & Kate Conger, *Russia Was Behind Cyberattack in Run-Up to Ukraine War, Investigation Finds*, N.Y. Times (May 10, 2022).

[9] AJ Vicens, *Top Ukrainian Cyber Official Praises Volunteer Hacks on Russian Targets, Offers Updates*, Cyberscoop (Mar. 15, 2022).

[10] Matt Burgess, *A Mysterious Satellite Hack Has Victims Far Beyond Ukraine*, Wired (Mar. 23, 2022).

[11] Joseph Marks, *11 Reasons We Haven't Seen Big Russian Cyberattacks Yet*, Wash. Post (Mar. 3, 2022).

[12] *See* Thomas Rid, Op-Ed., *Why You Haven't Heard About the Secret Cyberwar in Ukraine*, N.Y. Times (Mar. 18, 2022).

https://doi.org/10.1017/aju.2022.20 Published online by Cambridge University Press

Although cyber operations are highly secretive, some hints about defenses have spilled into public view. U.S. officials have noted "extensive work done to harden Ukraine's networks after Russian attacks on its electric grid in 2015 and 2016,"[13] and consistent with the announced U.S. "defend forward" policy,[14] media reports indicate that "[h]idden away on bases around Eastern Europe," U.S. Cyber Command "'cybermission teams' are in place to interfere with Russia's digital attacks and communications."[15] National Security Agency Director and Commander of U.S. Cyber Command Gen. Paul Nakasone recently told Congress, "We've worked very, very hard with Ukraine over the past several years," including having "'hunt forward' teams from US Cyber Command in Kyiv."[16] Defensive experience appears to be paying dividends, allowing authorities to prevent intrusions from causing damage. In April, the U.S. Department of Justice announced the disruption of a Russian government-controlled botnet *before* it was used,[17] and Ukrainian authorities successfully stopped an in-progress cyberattack by Russia's military intelligence agency before it could cause a blackout.[18]

Defenses are coming not just from governments, but also from companies.[19] For example, when Microsoft discovered wiper malware targeting Ukraine's government, within hours it not only updated its own systems to block the malware, but at the White House's request, shared the code with European governments.[20] Media reports suggest that "much of the actionable intelligence is being found by companies like Microsoft and Google, who can see what is flowing across their vast networks."[21]

In addition to blocking attacks, a different kind of defense comes from resilience. Even in the face of attempted and, in some cases, successful disruptions, Ukrainian government and civilian systems and networks have proven resilient, enabling fierce resistance to Russia. For example, civilians and officials in areas that have lost conventional internet have reportedly turned to Starlink satellite internet services, provided by Elon Musk, as has "a Ukrainian unit [that] is using Starlink to connect its drones attacking Russian forces."[22]

If successful defenses are at least part of the explanation for the absence of severe effects from cyber operations, then the Ukraine case study may serve as a counterpoint to the frequent mantra in cybersecurity that offense dominates defense. This is not to say that cyber defense will always prevail. It still frequently fails. Case-in-point: just last year the United States blamed Russia for successfully breaching numerous private sector and government agencies in the SolarWinds incident.[23] Nonetheless, perhaps Ukraine will show that experienced defenders engaging in *focused* defense of discrete known targets in a particular timeframe can succeed. Having a clear example of successful cyber defenses in such circumstances might spur the U.S. and allied governments to supercharge defensive assistance internationally (to say nothing of domestically). The North Atlantic Treaty Organization (NATO) has pledged continuing cybersecurity assistance to

[13] David E. Sanger, et al., *Arming Ukraine: 17,000 Anti-Tank Weapons in 6 Days and a Clandestine Cybercorps*, N.Y. Times (Mar. 6, 2022).

[14] U.S. Dep't of Defense, Summary: Department of Defense Cyber Strategy 1–2 (2018).

[15] Sanger, et al., *supra* note 13.

[16] Maggie Miller, *The World Holds Its Breath for Putin's Cyberwar*, Politico (Mar. 23, 2022).

[17] Kate Conger & David E. Sanger, *U.S. Says it Secretly Removed Malware Worldwide, Pre-empting Russian Cyberattacks*, N.Y. Times (Apr. 6, 2021).

[18] Andy Greenberg, *Russia's Sandworm Hackers Attempted Third Blackout in Ukraine*, Wired (Apr. 12, 2022).

[19] *See* Kristen E. Eichensehr, *Public-Private Cybersecurity*, 95 Tex. L. Rev. 467, 494–99 (2017).

[20] David E. Sanger, Julian E. Barnes & Kate Conger, *As Tanks Rolled Into Ukraine, So Did Malware. Then Microsoft Entered the War*, N.Y. Times (Feb. 28, 2022).

[21] *Id.*

[22] Rachel Lerman & Cat Zakrzewski, *Elon Musk's Starlink Is Keeping Ukrainians Online When Traditional Internet Fails*, Wash. Post (Mar. 19, 2022).

[23] *See* Kristen Eichensehr, *SolarWinds: Accountability, Attribution, and Advancing the Ball*, Just Security (Apr. 16, 2021).

https://doi.org/10.1017/aju.2022.20 Published online by Cambridge University Press

Ukraine,[24] and its Cooperative Cyber Defence Center of Excellence (CCDCOE) admitted Ukraine as a "contributing participant."[25]

The second broad explanation for the lack of significant cyberattacks is that Russia chose not to deploy them for any of several possible reasons. Perhaps expecting a quick victory with conventional forces, Russia chose not to engage in the detailed planning required for successful cyber operations.[26] Or perhaps Russia was deterred from attempting cyberattacks due to fears of cross-border spillover that could escalate into direct conflict with NATO.[27] Such spillover happened with NotPetya and the Viasat hack. If true, this explanation would be surprising because deterrence is generally thought to be weak with respect to cyber operations, and it might prompt a rethinking and retheorizing of how deterrence operates in cyberspace.[28] On the other hand, Russia seems largely undeterred by much else that the international community has mustered to date, so deterrence alone seems an unlikely explanation.

Another version of the story in which Russia chose not to attempt significant cyberattacks goes to the optimal role for cyber operations. Cyber operations have a significant comparative advantage over conventional force where they can enable espionage or stealthy intrusions, intended to be deniable or non-escalatory. But in a hot conflict, "[i]t's far easier to target the enemy with artillery, mortars and bombers than with exquisite and ephemeral cyber power."[29] The Ukraine invasion may drive this point home by showing that even when a major cyber power launches a war, major cyber-related disruption may not follow or not follow immediately. Of course, another country or conflict might proceed differently, using significant strategic cyberattacks and/or precisely targeted and timed cyber operations in support of battlefield troops. Russia's tactics may still change with respect to cyberattacks on Ukraine or abroad, as the United States continues to warn.[30] But future significant attempted and even successful Russian cyberattacks would not change the fact that the initial invasion played out differently than many expected.

Where Do We Go from Here?

The Ukraine conflict will undoubtedly offer lessons for technical experts and network defenders, but perhaps also for international lawyers and policy makers. In recent years, hypothetical major, destructive cyberattacks have attracted significant attention. But out-of-the-blue cyber Pearl Harbors or cyber 9/11s have not materialized,[31] and as Russia's invasion illustrates, even in an international armed conflict, "there is no cyber 'shock and awe'"—or at least not necessarily.[32]

What we do see, however, are lower-level cyber operations that are more consistent and consistently destabilizing. These operations are typical of the gray zone—the ambiguous strategic space between peace and open

[24] Statement by NATO Heads of State and Government (Mar. 24, 2022).

[25] Suzanne Smalley, *Ukraine, Looking to Fortify Itself Against Russian Attacks, Admitted to NATO Cyber Center*, CYBERSCOOP (Mar. 4, 2022).

[26] Marks, *supra* note 11.

[27] *Id.*

[28] *See, e.g.*, Max Smeets & Stefan Soesanto, *Cyber Deterrence Is Dead. Long Live Cyber Deterrence!*, COUNCIL FOR. REL. (Feb. 18, 2020) (chronicling critiques of and future directions for cyber deterrence research).

[29] Erica D. Lonergan, Shawn W. Lonergan, Brandon Valeriano & Benjamin Jensen, *Putin's Invasion of Ukraine Didn't Rely on Cyberwarfare. Here's Why.*, WASH. POST (Mar. 7, 2022).

[30] White House Press Release, Statement by President Biden on our Nation's Cybersecurity (Mar. 21, 2022).

[31] *See, e.g.*, Joseph Marks, *Cybersecurity Pros Want to Stop Talking about a "Cyber 9/11,"* WASH. POST (Sept. 10, 2021).

[32] Lennart Maschmeyer & Nadiya Kostyuk, *There Is No Cyber "Shock and Awe": Plausible Threats in the Ukrainian Conflict*, WAR ON THE ROCKS (Feb. 8, 2022).

https://doi.org/10.1017/aju.2022.20 Published online by Cambridge University Press

armed conflict. Examples include brief disruptions to critical infrastructure, DDOS attacks rendering websites inaccessible, ransomware, and intrusions into election infrastructure.[33] Such operations play to cyberattacks' strengths: fostering confusion about what has happened and who is responsible, allowing deniability for states to limit escalation, and causing insidious long-term loss of trust in digital systems and loss of competitiveness due to intellectual property theft. These kinds of operations keep relations simmering without boiling over. A crucial piece of such a strategy also involves masking state involvement, often by involving hackers with murky relations with states and thereby posing attribution challenges.

Part of what is significant about the Ukraine conflict is not just the absence of high-end mass destructive or disruptive cyberattacks, but also the *presence* of the DDOS and other operations typical of the gray zone—albeit at an apparently heightened rate.[34] The Ukraine conflict has also provided fresh examples of blurring of lines between state and non-state actors. Hackers have aligned themselves with both sides.[35] Ukraine's minister of digital transformation tweeted that the country was "creating an I.T. army," reportedly drawing thousands of participants who have taken Russian entities offline at times,[36] and on the opposite side, at least one ransomware group aligned itself with Russia, promising to retaliate against the West.[37] Such groups raise legal questions about state responsibility both during and outside of armed conflict.

From the perspective of international lawyers, the cyber aspects of the Russia-Ukraine conflict suggest the increased urgency of efforts by states, academics, and civil society to clarify legal rules applicable to both high-end and gray-zone-like cyber operations.[38] In some ways the legal frameworks for the high-end, major destructive cyberattacks are easier and further along. Many states appear to be coalescing around treating cyberattacks that produce consequences similar in scale and effects to conventional uses of force as equivalent to the conventional uses of force that they resemble.[39] But much more work remains to be done on the gray zone-like questions arising both outside and inside armed conflict. For some issues that means setting a rule—which cyber operations below the use of force threshold violate international law? Or what kinds of effects serve to qualify cyber operations as "attacks" for purposes of international humanitarian law?[40] For other issues, work remains on how to make existing rules—like the responsibility of states for non-state actors—effective in the cyber domain.

Developing more international rules after Russia's flagrant violations of the most sacrosanct of international law provisions on the use of force and territorial integrity may seem an ironic recommendation. But it is not. The Ukraine invasion has not (yet) escalated into a direct conflict between superpowers, and for this conflict and other operations outside international armed conflicts, greater clarity about the rules for cyber operations can help to avoid or at least manage escalation.[41]

[33] *Cf.* Michael N. Schmitt, *Grey Zones in the International Law of Cyberspace*, 42 YALE J. INT'L L. ONLINE 1 (2017).

[34] *See* David Cattler & Daniel Black, *The Myth of the Missing Cyberwar: Russia's Hacking Succeeded in Ukraine—And Poses a Threat Elsewhere, Too*, FOR. AFF. (Apr. 6, 2022); Dustin Volz & Robert McMillan, *In Ukraine, a "Full-Scale Cyberwar" Emerges*, WALL ST. J. (Apr. 12, 2022).

[35] Kate Conger & Adam Satariano, *Volunteer Hackers Converge on Ukraine Conflict with No One in Charge*, N.Y. TIMES (Mar. 4, 2022).

[36] *Id.*; *see also* Laurens Cerulus, *Kyiv's Hackers Seize Their Wartime Moment*, POLITICO (Mar. 10, 2022).

[37] Thomas Brewster, *A Ransomware Crew Pledged Allegiance to Russia. Now Its Data Has Been Leaked by a Pro-Ukraine Hacker*, FORBES (Feb. 28, 2022).

[38] *See, e.g.*, UN Open-Ended Working Group on Developments in the Field of Information and Telecommunications; NATO CCDCOE, CCDCOE to Host the Tallinn Manual 3.0 Process; Oxford Process on International Law Protections in Cyberspace.

[39] NATO CCDCOE, *Use of Force* (collecting state positions).

[40] *See* TALLINN MANUAL 2.0 ON THE INTERNATIONAL LAW APPLICABLE TO CYBER OPERATIONS 415–18 (Michael N. Schmitt gen. ed., 2017).

[41] *Cf.* Katrina Manson, *Biden Warns Cyber Attacks Could Lead to a "Real Shooting War,"* FIN. TIMES (July 27, 2021) (quoting Biden saying "If we end up in . . . a real shooting war with a major power, it's going to be as a consequence of a cyber breach").

https://doi.org/10.1017/aju.2022.20 Published online by Cambridge University Press