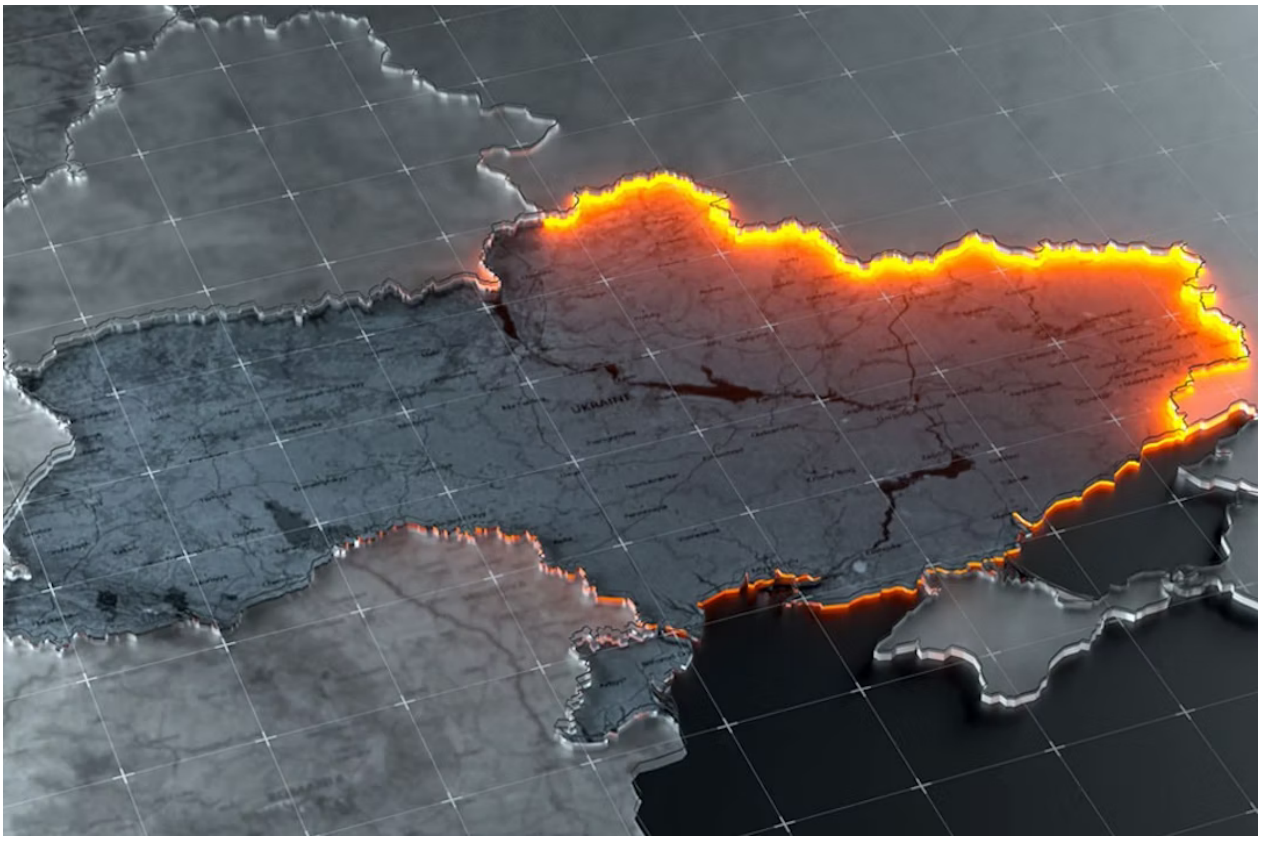
THIRD WAY

MEMO *Published April 25, 2022 • 12 minute read*

Hacking the Invasion: The Cyber Implications of Russia's Invasion of Ukraine



Aaron Clarke
Special Advisor to Communications and National Security

The Russian war on Ukraine has focused mostly on the kinetic dimensions of the conflict. But there are massive surprises, lessons and implications related to cyber. This paper covers the cyber component of the conflict and explores the implications that the invasion will have on:

- **Hacker Recruitment:** Previously apolitical cyber groups and hackers are now choosing sides in the conflict signaling a potential shift in how cyber groups recruit and behave going forward. In cyber, the implications are huge: "anyone can join a war."
- **UN Cybercrime Treaty:** Existing rifts between nations on the definition of criminal activity, digital sovereignty and free speech have widened and hardened as negotiations for a new cybercrime treaty commence amid the backdrop of war.

- **Bilateral U.S.-Russia Ransomware Talks:** Cyber diplomacy negotiations between the U.S. and Russia have stalled and attempts from Russia to restart talks could be fruitless or a smokescreen.

Cyber Attacks Since the Invasion

Expectations for severe cyber attacks on Ukraine have so far been overestimated. Just days prior to the invasion and bracing for a flurry of attacks, the European Union deployed a cyber rapid-response team to bolster Ukraine's cyber defenses and enhance cooperation during the conflict. [1] In January, Deputy National Security Advisor Anne Neuberger announced that the U.S. had been working with Ukraine to "harden their defenses." [2] The Biden administration has also sent out numerous warnings to American businesses to shore up their own cyber defenses from cyber attacks it still sees as impending. [3] In another concerted effort to shore up Ukraine's cyber defense capabilities, NATO took the step of accepting Ukraine as a contributing participant into the NATO Cooperative Cyber Defence Centre of Excellence (CCDCOE). [4]

Still, from the outset of the conflict, Russia has refrained from large-scale attacks targeting Ukraine's critical infrastructure. Russia is largely using distributed denial-of-service (DDoS) attacks on Ukrainian governmental and banking institutions, taking the websites' services offline for a few hours before having access restored. The cyber attacks on Ukraine started on January 13 [th] with the malware wiper attack, "Whispergate," maliciously deleting information on the Ukrainian Foreign Ministry and other Cabinet-level officials. [5] Russia would follow up with additional wiper attacks on Ukrainian governmental systems on the first two days of the invasion similar in nature and size of the January malware attack. [6] These attacks only constitute a fraction of the cyber capabilities Russia has used on Ukraine's critical infrastructure in the past, including disabling electrical grids across the country in 2015. [7]

Meanwhile, Ukraine and its volunteer "IT Army" along with other outside hacktivist groups like Anonymous have deployed their own wiper attacks. Made up of over 300,000 members from across the world organizing on social media websites, Ukraine's volunteer IT Army has taken aim at Russian critical infrastructure like its electrical grid and transportation services. [8]

Still, the level of cyber attacks currently deployed in the conflict is low compared to expectations. But it should not lull observers into a false sense of security. The current cyber path that Vladimir Putin is tracking now leaves considerable room for him to escalate if he feels it can change the tides of a stalling invasion. There are already signs that Russia is willing to escalate in the cyber realm with its "most severe" attack on one of Ukraine's largest telecommunications companies, Ukrtelecom, on March 28. [9] The attack disrupted internet connectivity for Ukrtelecom users before the company said it had "neutralized" the threat. The severity and target of the attack shows

Putin's willingness and ability to escalate the impact of cyber attacks on Ukraine and those supporting Ukraine.

This threat has not been lost on the U.S. and its allies, who are still wary of the potential escalation on the cyber front of the conflict. Most recently on March 21, President Biden warned American companies to prepare for cyber attacks from Russian hackers, advising them to "accelerate efforts to lock their digital doors." [10] Germany's Federal Office for Information Security (BIS), recently suggested that all German businesses using Kaspersky, Russia's leading antivirus software company, find replacement services due to the potential cybersecurity risks the Russian company posed. [11] And the British government's cybersecurity arm, the National Cyber Security Centre, issued a similar statement on March 29 th , recommending that British businesses "consider the risks" of using Russian-controlled products and services. [12]

Implications

Political Cyber and Hacker Recruitment

Pre-war, there was often a mercenary, though apolitical credo among many hackers and cyber groups. The motivation was often money, possibly disruption or perhaps some loose affiliation with a cause. There are signs this is changing.

In the years preceding the invasion, cyber intrusions originating from Russia were nothing new for Ukraine, which has been called "Russia's cyber playground" by intelligence officials in the past. [13] Armed with the cyber expertise of the Kremlin working alongside outside hacker groups, cyber attacks have plagued Ukrainian networks for years. These outside hacker groups have been responsible for some of the more debilitating ransomware attacks on foreign networks and companies that have brought in large sums of money.

But the invasion of Ukraine may be altering the decision-making calculus of hacker groups going forward when it comes to recruitment in ways that may be lasting. Previously driven by profit from collecting ransom payments, these hacker groups are now being deployed in an armed conflict for the sake of their country or a country for whom they have grown affinity. In their global incident report, IT consulting firm Accenture describes how previous norms between hacker groups in the region are eroding and splitting groups along conflict lines. [14] Previously refraining from conducting cyber attacks within the Commonwealth of Independent States (CIS) (a group of nine former Soviet states including Russia) the conflict has pitted hackers against one another in support of or against Russia.

The decision of whether to let ransomware hackers back into Russian underground online forums is also dividing groups, with their potential re-admission leading to further "emboldened" hackers taking part in the conflict. With these divides getting deeper and deeper as cyber attacks and the conflict continue, it could change recruiting on two fronts in the future.

The first front revolves around whom these hacker groups target as recruits and why. The splintering of these groups and potential lack of agreed upon norms going forward means whom these groups accept and for what reasons could change. Instead of accepting someone with the cyber expertise to carry out attacks, groups may start requiring that a certain political allegiance be held for admission or serve as the main driving force behind recruitment. In an interview with Politico, Howard Marshall, the managing director of Accenture and former deputy assistant director of the FBI's cyber division, said that in lieu of money, hackers might join if "think they have a cause worth fighting for." [15]

In the future, even absent a conflict, cyber attacks can start to take on more and more of a role as a political tool rather than a weapon used by criminal actors. While cyber intrusions as a political tool aren't new, with Russia's election interference of the 2016 U.S. presidential election being a prime example, outside hacker groups could start to form for purely political reasons, with or without explicit state support.

The second front is the proliferation of hackers joining Ukraine's volunteer IT Army. The Ukrainian government has voiced its support for the actions of the social media-organized group, but it has also made clear they are not directly working in unison with them. [16] Its more than 300,000 members are based across the globe with some having no ties to the conflict at all. The rogue nature of the group means that the threat for miscalculation from an outside group could unnecessarily escalate the cyber side of the conflict. [17] While the Ukrainian government can voice its concern or objections to certain "tasks" the group assigns, there's nothing stopping the group from either carrying out an attack without their approval or preventing offshoots from the group acting outside the given objectives.

This also threatens to proliferate in future conflicts, where countries rely on outside actors to provide cyber support against their adversary or outside actors feel the need to get involved on one side or the other. Lotem Finkelstein, head of threat intelligence at Check Point Software, summed it up when he said, "for the first time in history anyone can join a war," and this trend of volunteer cyber armies could just be in its early stages. [18]

UN Cybercrime Treaty and the meaning of "crime"

On February 28, while the invasion was just underway, the United Nations began a three-year long process of negotiating a proposed cybercrime treaty that could have far reaching implications for how cybercrime is tackled internationally. [19] Spearheaded by Russia, the push for a new treaty comes with a number of contentious talking points like international cooperation, digital sovereignty, access to data, and how to even define what a "cybercrime" is. [20] Sides have begun to take shape that favor different sized scopes or competing definitions with the invasion of Ukraine potentially spilling over into a couple of areas.

One of the core issues is as the definition of a "cybercrime" and the implications it has for how it's enforced. [21] Last year in the lead up to negotiations, the EU and Russia submitted competing interpretations on what direction the definition should go in. In their provisional treaty draft submitted in July 2021, Russia wanted cybercrime to expand into "other unlawful acts motivated by political, ideological, social, racial, ethnic, or religious hatred" that only have to be cyber-related in nature. [22] With a narrower, "cyber-dependent" definition where the crime has to "threaten the confidentiality, integrity, and availability of data and systems," the EU plan would prevent the sort of expansionist stance that Russia submitted, that could make something like protesting the invasion online a cybercrime. This comes at a time when Russian human rights groups are reporting spikes in arrests of anti-war protesters. [23]

The question of "digital sovereignty" is also expected to play out as Ukraine's physical sovereignty is encroached. [24] Unlike defining what constitutes as a cybercrime, this sticking point does not find its differences in action. Most UN countries have pushed for greater control or sovereignty over data originating within their borders. European Commission President Ursula von der Leyen in February 2020 called for greater "tech sovereignty" so that Europe "make its own choices, based on its own values, respecting its own rules." [25] Concerns arise from what is done with that sort of control over data. More authoritarian states like Russia or China could use this to expand on their already growing digital surveillance apparatuses. This issue becomes even murkier considering the territorial claims that Russia has made regarding the invasion and claims to the Donetsk and Luhansk regions. As the vast majority of UN member states voice their opposition to the invasion of Ukraine, it has already made its way into negotiations, with an EU representative saying, "these cyberattacks are not conducive to a constructive engagement with Russia on this treaty." [26]

This suggests the invasion itself could also play a role in how negotiations progress. The international backlash has been swift and sweeping from UN members who will have to sit across from their Russian counterparts and draft this treaty. With a target end date in 2025, the treaty process is still in its very nascent stages and negotiations began in the backdrop of this conflict, so concerns of the conflict derailing talks would be premature. Still, the low-level cyber activity currently being deployed by Russia against Ukraine suggests that there could still be room for more impactful cyberattacks that shake the international landscape for talks.

Bilateral U.S.-Russia Ransomware Talks

After previous discussions in 2021 and 2022 were held by President Biden and Vladimir Putin to address the issue of ransomware originating from Russian hacker groups, communication between the two on cyber diplomacy has ceased in the wake of the invasion. [27] On March 14, Russia's Deputy Foreign Minister, Oleg Syromolotov, announced that Russia hoped to renew the talks between the two countries to build off of the Geneva Summit in June 2021, but it seems very unlikely the Biden administration will accept. [28] The likelihood of an agreement between the two countries on some sort of framework on cybersecurity was low to begin with, with Russia's cyber envoy Andrey

Krutskikh in December 2021 saying negotiations within the UN on cyber diplomacy were "proceeding with great difficulty." [29] But the added layer of the invasion will only further complicate any efforts on fighting ransomware in the future.

There are some observers who feel the United States should open a channel of dialogue with its Russian counterparts and take up Deputy Foreign Minister Syromolotov's offer of renewed talks. With the ongoing deterioration of U.S.-Russia relations due to devastating sanctions and U.S. support for Ukraine, the idea would be that having an open channel on at least one issue would ensure that communication does not go completely dark during the conflict. [30] With previous talks not garnering much progress and the U.S. continuing to provide material and logistical support to Ukraine, any attempts to restart talks will probably be ignored or seen as a "distraction." [31]

President Biden's March 21 st warning to American companies to secure their networks also signals the Administration's feelings on Russia's commitment to tamping down cyber attacks. The impact from sanctions is expected to be felt long-term by the Russian economy, making the companies complying with them targets for the foreseeable future as well. Russia's questionable positions on the UN Cybercrime Treaty shows it's still set on having broader norms established that would favor Russia's authoritarian behavior online. The three-page UN cyber norms agreement that both countries signed on to this past November was seen as a positive step at the time, but the erosion of relations between the countries since the invasion will hinder attempts to reestablish negotiations. [32]

Conclusion

The ripple effects of the Russian invasion of Ukraine are expected to be felt as the conflict stretches on further into the spring and summer. Uncertainty around the length and destruction of the invasion will continue to change the dynamics of the conflict and could alter how the cyber side of the conflict is currently playing out. While the "all-out" cyber warfare from this conflict has not arisen yet, its impact in different areas of cybersecurity will be felt in future conflicts to come.

TOPICS

CYBERSECURITY 98

ENDNOTES

1. Tidy, Joe. "Ukraine: EU deploys cyber rapid-response team." *BBC News*, 22 Feb. 2022, https://www.bbc.com/news/technology-60484979, accessed 11 Apr. 2022.

2. Lyngaas, Sean. "US officials prepare for potential Russian cyberattacks as Ukraine standoff continues." ABC12 News, 2 Feb. 2022. https://www.abc12.com/us-officials-prepare-for-potential-russian-cyberattacks-as-ukraine-standoff-continues/article_7caece66-78b1-5cdd-8c42-194517949356.html, accessed 11 Apr. 2022.

3. Reuters. "U.S. warns defense contractors about possible Russian cyber attacks." *Reuters*, 2 Feb. 2022. https://www.reuters.com/world/us-warns-defense-contractors-about-possible-russian-cyber-attacks-2022-02-16/, accessed 11 Apr. 2022.

4. NATO Cooperative Cyber Defence Centre of Excellence. "Ukraine to be accepted as a Contributing Participant to NATO CCDCOE." *NATO Cooperative Cyber Defence Centre of Excellence*, 4 Mar. 2022. https://ccdcoe.org/news/2022/ukraine-to-be-accepted-as-a-contributing-participant-to-nato-ccdcoe/, accessed 11 Apr. 2022.

5. Fendorf, Kyle and Jessie Miller. "Tracking Cyber Operations and Actors in the Russia-Ukraine War." *Council on Foreign Relations*, 24 Mar. 2022. https://www.cfr.org/blog/tracking-cyber-operations-and-actors-russia-ukraine-war, accessed 11 Apr. 2022.

6. Fendorf, Kyle and Jessie Miller. "Tracking Cyber Operations and Actors in the Russia-Ukraine War."

7. Finkle, Jim. "U.S. firm blames Russian 'Sandworm' hackers for Ukraine outage." *Reuters*, 7 Jan. 2016. https://www.reuters.com/article/us-ukraine-cybersecurity-sandworm-idUSKBN0UM00N20160108, accessed 11 Apr. 2022.

8. Fendorf, Kyle and Jessie Miller. "Tracking Cyber Operations and Actors in the Russia-Ukraine War."

9. Brewster, Thomas. "'Most Severe' Cyberattack Since Russian Invasion Crashes Ukraine Internet Provider." *Forbes*, 28 Mar. 2022. https://www.forbes.com/sites/thomasbrewster/2022/03/28/huge-cyberattack-on-ukrtelecom-biggest-since-russian-invasion-crashes-ukraine- telecom/?mc_cid=b66880d100&mc_eid=35d2427271&sh=cba4a477dc28, accessed 11 Apr. 2022.

10. Gill, Jaspreet. "Biden tells private sector to 'lock their digital doors' before Russia gets in." *Breaking Defense*, 21 Mar. 2022. https://breakingdefense.com/2022/03/biden-tells-private-sector-to-lock-their-digital-doors-before-russia-gets-in/, accessed 11 Apr. 2022.

11. Cerulus, Laurens. "German cyber agency: Rip Kaspersky out of your systems." *Politico*, 15 Mar. 2022. https://subscriber.politicopro.com/article/2022/03/german-cyber-agency-rip-kaspersky-out-of-your-systems-00017275, accessed 11 Apr. 2022.

12. Levy, Ian. "Use of Russian technology products and services following the invasion of Ukraine." National Cyber Security Centre, 29 Mar. 2022. https://www.ncsc.gov.uk/blog-post/use-of-russian-technology-products-services-following-invasion-ukraine, accessed 11 Apr. 2022.

13. The Economist. "Will war in Ukraine lead to a wider cyber-conflict?" *The Economist*, 23 Feb. 2022. https://www.economist.com/europe/2022/02/23/will-war-in-ukraine-lead-to-a-wider-cyber-conflict, accessed 11 Apr. 2022.

14. Accenture. "Global Incident Report: Threat Actors Divide Along Ideological Lines over the Russia-Ukraine Conflict on Underground Forums." *Accenture*, 14 Mar. 2022. https://acn-marketing-blog.accenture.com/wp-content/uploads/2022/03/UPDATED-ACTI-Global-Incident-Report-Ideological-Divide-Blog-14MARCH22.pdf, accessed 11 Apr. 2022.

15. Sabin, Sam. "Passing cyber reporting rules was just the first step." *Politico*, 14 Mar. 2022. https://www.politico.com/newsletters/weekly-cybersecurity/2022/03/14/passing-cyber-reporting-rules-was-just-the-first-step-00016891, accessed 11 Apr. 2022.

16. Gill, Jaspreet. "Why Ukraine recruiting amateur 'IT army' could backfire." *Breaking Defense*, 2 Mar. 2022. https://breakingdefense.com/2022/03/why-ukraine-recruiting-amateur-it-army-could-backfire/, accessed 11 Apr. 2022.

17. Gill, Jaspreet. "Why Ukraine recruiting amateur 'IT army' could backfire."

18. Pitrelli, Monica Buchanan. "'For the first time in history anyone can join a war': Volunteers join Russia-Ukraine cyber fight." *CNBC*, 14 Mar. 2022. https://www.cnbc.com/2022/03/14/volunteers-sign-up-to-help-in-cyberwars-between-russia-and-ukraine-.html, accessed 11 Apr. 2022.

19. United Nations Office on Drugs and Crime. "First session of the Ad Hoc Committee." *United Nations Office on Drugs and Crime*, 28 Feb. 2022. https://www.unodc.org/unodc/en/cybercrime/ad_hoc_committee/ahc-first-session.html, accessed 11 Apr. 2022.

20. Walker, Summer. "The Quixotic Quest to Tackle Global Cybercrime." *Foreign Policy*, 11 Feb. 2022. https://foreignpolicy.com/2022/02/11/un-cybercrime-treaty-russia-hacking/, accessed 11 Apr. 2022.

21. Walker, Summer. "The Quixotic Quest to Tackle Global Cybercrime."

22. United Nations Office on Drugs and Crime. "United Nations Convention on Countering the Use of Information and Communications Technologies for Criminal Purposes." *United Nations Office on Drugs and Crime*, 29 Jun. 2021. https://www.unodc.org/documents/Cybercrime/AdHocCommittee/Comments/RF_28_July_2021_-_E.pdf, accessed 11 Apr. 2022.

23. "Anti-war protests intensify in Russia along with police crackdown." *Al-Jazeera*, 10 Mar. 2022. https://www.aljazeera.com/news/2022/3/10/anti-war-protests-intensify-in-russia-along-with-police-crackdown, accessed 11 Apr. 2022.

24. Walker, Summer. "The Quixotic Quest to Tackle Global Cybercrime."

25. von der Leyen, Ursula. "Shaping Europe's digital future: op-ed by Ursula von der Leyen, President of the European Commission." *European Commission*, 19 Feb. 2020. https://ec.europa.eu/commission/presscorner/detail/en/AC_20_260, accessed 11 Apr. 2022.

26. Rodriguez, Katitza and Karen Gullo. "Negotiations Over UN Cybercrime Treaty Under Way in New York, With EFF and Partners Urging Focus on Human Rights." *Electronic Frontier Foundation*, 3 Mar. 2022. https://www.eff.org/deeplinks/2022/03/negotiations-over-international-police-powers-agreement-must-keep-human-rights, accessed 11 Apr. 2022.

27. Sabin, Sam. "Debriefing Russia's 'strange' request to jumpstart U.S. cyber talks." *Politico*, 15 Mar. 2022. https://subscriber.politicopro.com/newsletter/2022/03/debriefing-russias-strange-request-to-jumpstart-u-s-cyber-talks-00017185, accessed 11 Apr. 2022.

28. "The Russian Foreign Ministry expects that dialogue with the United States on cybersecurity will be restored." *TASS*, 14 Mar. 2022. https://tass.ru/politika/14063755?utm_source=subscriber.politicopro.com&utm_medium=referral&utm_campaign=subscriber.politicopro.com&utm_referrer=subscriber.politicopro.com, accessed 11 Apr. 2022.

29. Kass, D. Howard. "Cybersecurity Talks Between U.S., Russia 'Proceeding with Great Difficulty,' Envoy says." *MSSP Alert*, 20 Dec. 2021. https://www.msspalert.com/cybersecurity-news/united-states-russia-negotiations/, accessed 11 Apr. 2022.

30. Sabin, Sam. "Debriefing Russia's 'strange' request to jumpstart U.S. cyber talks."

31. Sabin, Sam. "Debriefing Russia's 'strange' request to jumpstart U.S. cyber talks."

32. Sherman, Justin. "The U.S. and Russia Might Finally Be Making a Tiny Bit of Progress on Cybersecurity." *Slate*, 11 Nov. 2021. https://slate.com/technology/2021/11/russia-us-cyber-norms-agreement-general-assembly.html, accessed 11 Apr. 2022.