LAWFARE

CYBER & TECHNOLOGY

Cyberwar in Ukraine: What You See Is Not What's Really There

By **Susan Landau** Friday, September 30, 2022, 8:01 AM

It has been seven months since Russia invaded Ukraine. Despite much speculation, many aspects of the war have ultimately not turned out as expected. The war wasn't, as Russia had anticipated, a six-day rout—or even a six-month one. And notably, cyber didn't, as some had predicted, play a major role in Russian efforts to take over Ukraine. Russia was expected to wage cyberattacks targeting critical infrastructure; its attacks, while sophisticated, have had less impact than envisioned. Meanwhile, even in the middle of what is turning out to be a more demanding war than Russian leadership had anticipated, Russia is focusing on a strategy of undermining the West through information warfare. This war has demonstrated strategic cyber issues below the surface, including the failure of effective cyberattacks occurring alongside kinetic offensives, Russia's long-term use of information warfare, and effective collaboration between U.S. industry and the U.S. government in preventing the worst of the cyberattacks. These have important long-term implications for the international defense strategies of the United States and other Western democracies.

For several years before Russia's invasion, Ukraine served as Russia's testbed for cyberattacks. In December 2015, Russian hackers launched a cyberattack that took down three regional electric power distribution networks in western Ukraine, leaving 225,000 people without power for several hours during cold winter conditions. What was striking about this particular attack is that the three grids were disabled within a half hour of each other. The grids were unconnected, and so these breakdowns were not the result of cascading failures, a not-uncommon situation for power grids. Thus this attack demonstrated an unexpected level of capability—by Russia or others. Launching such nearly simultaneous attacks against three distribution networks that each operated somewhat differently had not been anticipated by the U.S. It was a wake-up call for the U.S. Department of Homeland Security, which worked to develop greater resiliency in the nation's power grids.

Over the next year, Ukraine faced an increasing series of cyberattacks against the private sector and government ministries. Almost exactly a year after the 2015 attack that disabled the three regional electric power distribution networks, Ukraine suffered another attack on its power grid. Employing far more sophisticated tools than the previous one, the 2016 attack took out a Kyiv transmission system—and had been intended to do even more damage. Then, in 2017, Russia launched the NotPetya attack, introducing malware into widely used Ukrainian tax software. But this cyberattack was not targeted—the software ignored whether a machine was located in Ukraine or using the Cyrillic alphabet—and it spread rapidly around the world. Wired reported this attack had devastating financial and operational effects on the Danish shipping giant Maersk, whose ships transported almost a fifth of the world's goods, Merck, FedEx's European subsidiary TNT Express, and multiple other companies. The Russian-based hackers seemed not to care about the worldwide impact of their attack—or perhaps that international impact was part of the intent.

Given Russia's extensive history of cyberwarfare in Ukraine, it seemed likely that cyberattacks would play a large role in Russia's war against Ukraine—and potentially against some of Ukraine's supporters, including NATO member states. But that is largely not what happened. The cyberattacks that Russia has executed since the start of its war against Ukraine are perhaps more accurately characterized by Ciaran Martin as "cyber harassment" since they have failed to occur at the strength many had anticipated.

Nadiya Kostyuk and Erik Gartzke have written a trenchant analysis of the expected cyberwar that didn't happen in Ukraine. They start by noting that cyber conflict can be a substitute for war—such as Stuxnet (which destroyed centrifuges at the Natanz nuclear facility, thus delaying Iran's progress toward building a nuclear weapon)—and also as a complement to kinetic warfare —such as the cyberattacks against Georgia in 2008 that brought down a number of Georgian government websites.

But Kostyuk and Gartzke also observe the difficulty of coordinating cyberattacks with kinetic warfare—especially on an ever-changing and unpredictable battlefield (which was certainly the state in the first weeks of the Ukrainian war). The difficulty of navigating these challenges should not be underestimated. Approximately one hour before Russia began its land invasion, it launched a major cyberattack against Viasat, a satellite internet company used by the Ukrainian military for command and control. The cyberattacks created communication outages in Ukraine and other European countries, including preventing remote control of German wind turbines. These cyberattacks, which were executed before Russian troops invaded Ukraine, did not disrupt Russia's own military forces. But launching such attacks during active warfare, when Russian forces have entered the battlefield and the impact on their own forces might be harder to determine, is quite another—and makes cyber, at least currently, a difficult tool to employ in the heat of battle.

Boots on the ground remain the most effective way to capture territory, which is the central aim of Russia's invasion. As Kostyuk and Gartzke explained, cyber provided "indirect complementarity," with kinetic warfare by using the internet to gather intelligence on Ukrainian and Western governments and also to disseminate disinformation campaigns against their populations. Their argument is correct. But it appears that there is more to the story of the role of cyber in the Russian war against Ukraine.

There were serious cyberattacks attempted against Ukraine. Before the start of its invasion of Ukraine, Russia launched a cyberattack that targeted Ukrainian government and financial websites. This attack—known as FoxBlade—was poised to wipe data from computers, crippling them. If FoxBlade received less attention than the Viasat attack, it's likely because the attack failed. Within hours of its appearance, the Microsoft Threat Intelligence Center had written code to stop it, which it quickly shared with the Ukrainian government.

What happened next represents an important change in the cooperation between the U.S. government and the tech industry: Microsoft informed Ann Neuberger, U.S. deputy national adviser for cyber and emerging technology, of the issue. Neuberger suggested that Microsoft share this information, including the code to disable FoxBlade, with other European governments, including in the Baltics and Poland, to prevent Russia from launching a FoxBlade attack against any other countries. Neuberger made the introductions. Microsoft shared the necessary information. Problem averted.

Recall that a decade ago, in the wake of the Edward Snowden disclosures, Silicon Valley and Washington were very much on the outs with each other. The relationship between Big Tech and Washington is different now. As Brad Smith, Microsoft's president and vice chair, explained in a blog post:

> [I]t's important to note that we are a company and not a government or a country. In times like this, it's especially important for us to work in consultation with those in government and, in this instance, our efforts have involved constant and close coordination with the Ukrainian government, as well as with the European Union, European nations, the U.S. government, NATO and the United Nations.

Microsoft was not the only U.S. company aiding Ukraine. Days before the invasion, Ukraine's government amended its data protection laws to permit data to move to the cloud. Before this change, Ukrainian public-sector digital infrastructure was run on servers within Ukraine—leaving the physical servers vulnerable to destruction by Russian missile attacks. Three days after Russian forces began their invasion of Ukraine, Amazon had delivered Snowball devices to Ukraine; these hardened devices were used to securely transfer Ukrainian government data to the cloud. According to Microsoft, within 10 weeks of the beginning of the war, many of the government's most important digital operations and assets had been moved to the cloud—and out of the war zone.

At the start of the invasion, many observers speculated that the Russians would aim to inflict cyberattacks on Ukrainian communications infrastructure. The attack on Viasat was a step in this direction. This attack was aimed to disable thousands of satellite modems across Europe. It created serious short-term harm by causing "a really huge loss in communications in the very beginning of the war," according to a top Ukrainian cybersecurity official. While temporarily crippling, the attack notably caused no long-term damage to European communications infrastructure. Since Russian forces' initial attack on Viasat and subsequent airstrike on a Kyiv television and radio broadcasting tower, they have not really taken aim at Ukrainian communications infrastructure.

This is due to Russian miscalculations. After having developed modern secure battlefield communications systems, Russian military personnel were unable to deploy them during their forces' battle to capture Kyiv. Russian military leadership had not anticipated the fierce Ukrainian defense they ran into. When they did, the Russian military was unwilling to use their new sensitive communications equipment lest it be captured by enemy forces. So Russian forces were compelled to rely on the Ukrainian communications systems to be working in order to communicate among themselves.

A reliance on Ukrainian systems wasn't the only problem that Russian forces encountered with their communications. Elsewhere, such as around Kharkiv, the Russian military made a serious strategic mistake. Early in the invastion, Russian forces bombed and shelled Ukrainian 3G and 4G cell towers—but these were necessary for transmitting encrypted communications. The Russians had shot themselves in the foot, as in those locations, their military forces were no longer able to use their advanced communications systems. Instead Russian military forces had to use less advanced—and unencrypted—channels. This misstep allowed Ukrainian forces to listen in on Russian communications and plan and respond accordingly.

Russia's long-term intentions also contributed to the lack of their destruction of Ukrainian communications infrastructure. Just as Russia had done in Crimea in 2014, Russia's plan was to quickly disconnect the population in conquered territory from Ukrainian communications networks and connect them instead to Russian ones following military victories in towns and cities. Russia executed this practice successfully in May after their forces captured the port city of Kherson in southern Ukraine.

Once the Ukrainian networks were rerouted to Russia systems, Russia planned to conduct the same communications surveillance and censorship it was imposing on its own population as well as to disseminate pro-Russia propaganda. Rebuilding and replacing destroyed Ukrainian communications infrastructure would have been expensive and delayed the shift. Russian strategists had expected a quick victory over their smaller neighbor, and thus wholesale replacement of Ukrainian communications infrastructure with Russian-built infrastructure was simply not in Russia's military playbook. So although Russian military forces do attack Ukrainian communications networks, it is much better for the Russian forces to have working infrastructure during their time in Ukraine than to disable the existing networks—limiting their own communications—and then having to replace them.

There is more to this story. U.S. Cyber Command also had a hand in preventing more serious Russian cyberattacks. Gen. Paul Nakasone, commander of U.S. Cyber Command, stated that the U.S. had been "[c]oordinating with the Ukrainians in an effort to help them harden their networks[.]" It is unknown what Cyber Command is doing to assist Ukraine; Nakasone declined to specify details of the U.S.-Ukraine coordination.

Russia's war in Ukraine reveals three lessons about how cyberwarfare may be incorporated into international conflict.

First, Russia is not, as some have said, less good at cyberwarfare than expected. Rather—as Kostyuk and Gartzke observed—cyber was not suitable for this situation. Russian cyberattacks are generally well honed. Microsoft's Brad Smith stated that "recent and ongoing [Russian] destructive attacks themselves have been sophisticated and more widespread than many reports recognize." The Canadian Centre for Cyber Security said precisely the same thing, noted Russia's increased espionage against NATO member nations, and stated that "Russia is almost certainly in the process of developing cyber capabilities against targets in the European Union and NATO, including the United States and Canada." Another reason for the lack of advanced and effective Russian cyberwarfare in Ukraine may be that Ukraine's defenses benefited from help, not only from U.S. Cyber Command but also from the European Union and the Five Eyes.

Second, Russia's military and political ambitions extend far beyond Ukraine. Russia's war against Ukraine is not just a war to take over the nation's territory; it is also a battle against the West. In June, Microsoft's Smith noted that:

> Russia's strategy—a long-term one, but highly visible here—involves cyber influence operations targeting democracies around the world. In the short term, the intent was to diminish international support for Ukraine, and there were some efforts in this direction.

For example, to justify their invasion, Russia planted stories that Ukraine had established a bioweapons lab with U.S. assistance. But another very real target of Russia's information warfare is the stability of the allied governments themselves.

Information warfare is a century-old strategy employed by both the Soviet Union and Russia. They are experts in it. And it is important not to underestimate Russia, which often changes tactics with each attack. As an example, consider Russia's efforts to disrupt U.S. elections. In 2016, Russia attacked U.S. elections by stealing Democratic National Committee emails and then arranging to have them released at opportune moments. In 2020, the Russians turned to trolls, bots, and fake news to bolster President Trump's chances of reelection—but also to create increased distrust in the voting process.

As Stephen Blank has written, Russia is simply following "the logic of past Soviet and Russian political warfare." This includes a four-pronged strategy of information operations, and they are following it strictly in Ukraine. The strategy includes tight control within Russia on information regarding the war (spreading information criticizing Russian efforts results in heavy prison sentences), propaganda within Ukraine aimed at undermining the population's support of their nation's government and efforts, information warfare aimed at Western audiences in an effort not just to diminish support for Ukraine but to sow disunity and destabilize governments at home, and information operations in nonaligned countries aimed at disparaging democracies.

Russian information warfare efforts in destabilizing Western nations extends well beyond messing with elections and weakening support for Ukraine. It includes going after the heart of democracies by undermining civil society. Online attacks on the January 2017 Women's March provide an early example of the Russian efforts to sow dissent within U.S. civil movements. The New York Times reported that Russian trolls targeted a Palestinian American who was one of the march's four co-leaders. The posts put up by trolls claimed she "was a radical Islamist, 'a pro-ISIS Anti USA Jew Hating Muslim' who 'was seen flashing the ISIS sign'." The result, not unexpectedly, was a fracturing of the march's leadership after what had been a harmonious and effective march.

Such activities have increased in recent years. Indeed, the intelligence community recently reported that Russia has given at least $300 million to Western political parties, officials, and politicians in order to "to shape foreign political environments in Moscow's favor." Using foundations, think tanks, and shell companies, the Russians funnel funding to support far-right nationalist parties. The intent of the effort is to fracture democracies' cohesion.

A June 2022 Microsoft report described some of these activities in detail. Microsoft estimates that U.S. consumption of Russian propaganda averages approximately 60-80 million page views a month; that puts it on par with how much the Wall Street Journal is read. What are Americans seeing on those pages? For example, while RT—Russia's state-controlled international news network—reported in Russian that "[l]ockdowns and boosters prevent transmission" of the coronavirus, RT in English stated that "[v]accinations fail to curb transmission … and have dangerous side effects." When such stories reach the United States, they transform initial doubts about vaccines into much stronger distrust—and not just of the vaccines, but of the government that promotes them. Microsoft found an increase in traffic from Russian news outlets to New Zealand pushing stories about "life-threatening side effects" of coronavirus vaccines. A month later, protests erupted against vaccination in the New Zealand capital.

Microsoft noted a similar unusual spike in Russian news traffic to Canada in January 2022 (usually the traffic trend lines for the U.S. and Canada look much the same, but that month the lines diverged). Here, the issue was the trucker convoy to Ottawa protesting Canadian coronavirus restrictions. The Russian articles presented a heightened sense of a government in crisis along with a lack of Canadian news coverage of the convoy. Russian propaganda and its amplification in other nations sharply increase internal tensions and distrust within targeted—most often Western—nations, which is exactly the long-term result Russia seeks.

Such Russian disinformation efforts should not be a surprise. Both Russia and China have long viewed Western commitments to open networks and free speech as a form of information warfare, and have consequently resisted negotiations with the West on curbing cyberwarfare in favor of discussions instead on curbing information warfare. Now Russia is actively employing information warfare techniques on the world during its war on Ukraine.

Russia is playing the long game in disrupting Western democracies; we can expect more of this type of information warfare in the future. Though researchers are discovering tools to "inoculate" against the dangers of information warfare, as Jack Goldsmith and Stuart Russell have observed, this form of attack is not easy for the United States and other Western democracies to overcome. As Goldsmith and Russell point out, the very strengths of U.S. society—private-sector global economic dominance, digital connectedness, free and open society, government transparency, and regulatory skepticism—greatly increase the nation's vulnerability to information warfare efforts by allowing its easy spread.

If these first two observations about the war are not that surprising, the third one—burgeoning cooperation between the U.S. government and U.S. industry on handling attacks—is both unexpected and extremely important.

The effort forged by Neuberger to share information disabling the FoxBlade attack with European governments was not simply a lucky accident. It grew out of a policy that the Biden administration strongly pursued. As National Cyber Director Chris Inglis put it at a meeting in June 2022:

> We often overestimate what a government would know, underestimate what the private sector knows, and ignore at our peril what we could know together. … We're looking for a degree of professional intimacy such that we can discover things together that no one of us could discover alone.

U.S. intelligence agencies are essentially saying, "Let us work genuinely together," rather than, "Tell us what you know, and we'll add it."

This change of viewpoint is a remarkable one for the U.S. government's approach; it's also appropriate and smart. Seven of the 10 largest cloud providers are U.S. based. By working together, the U.S. government can gain access to real-time information they're gleaning about network flows to spot trouble early. The government and technology companies can share information about the anomalies and problems discovered independently, to diagnose and address threats as they arise. As Inglis has said, "You put subject matter experts from the private and public sector together to say let's share our insights because we need to be able to discover this tactical warning as it happens."

This represents an extremely positive and important step toward combating cybersecurity threats. But notably, companies will likely collaborate with the government only if it serves their interests—and if they choose to do so, they must not undermine their primary effort of protecting their customers (in other words, no co-opting private customer data for other purposes). This effort will likely be a complicated dance, but it is one that U.S. intelligence agencies have recognized is important to get right. This cooperation is a valuable arrow in the West's quiver. It is also one that Russia lacks. Some other adversaries, including China, do have this capability, though not to the extent that the United States does. Despite this difference, the threat posed by Russia's willingness to wage information warfare at high scale should not be underestimated. Russia's highly destabilizing strategy has arrived at a moment when Western democracies are already under threat.

Though cyberwarfare did not occur as anticipated in Russia's war against Ukraine, it has played an important role from the start. The engagements in cyberwar have left the United States and its allies with two challenges: determining how to handle information warfare and developing an understanding of how the particular set of actions in this war change our perception of how cyberwar might—or might not—take place in future conflicts.

Topics: Russia-Ukraine War, Cyber & Technology, Russia and Eastern Europe

Tags: cyberwar, Russia-Ukraine War

Susan Landau is Bridge Professor in The Fletcher School and Tufts School of Engineering, Department of Computer Science, Tufts University and Visiting Professor, University College London, Department of Computer Science. She

directs Tufts MS program in Cybersecurity and Public Policy. Her most recent book, "People Count: Contact-Tracing Apps and Public Health," was published by MIT Press in 2021. Landau has testified before Congress and briefed U.S. and European policymakers on encryption, surveillance, and cybersecurity issues. Landau is a member of the Cybersecurity Hall of Fame, a fellow of the American Association for the Advancement of Science and of the Association for Computing Machinery.