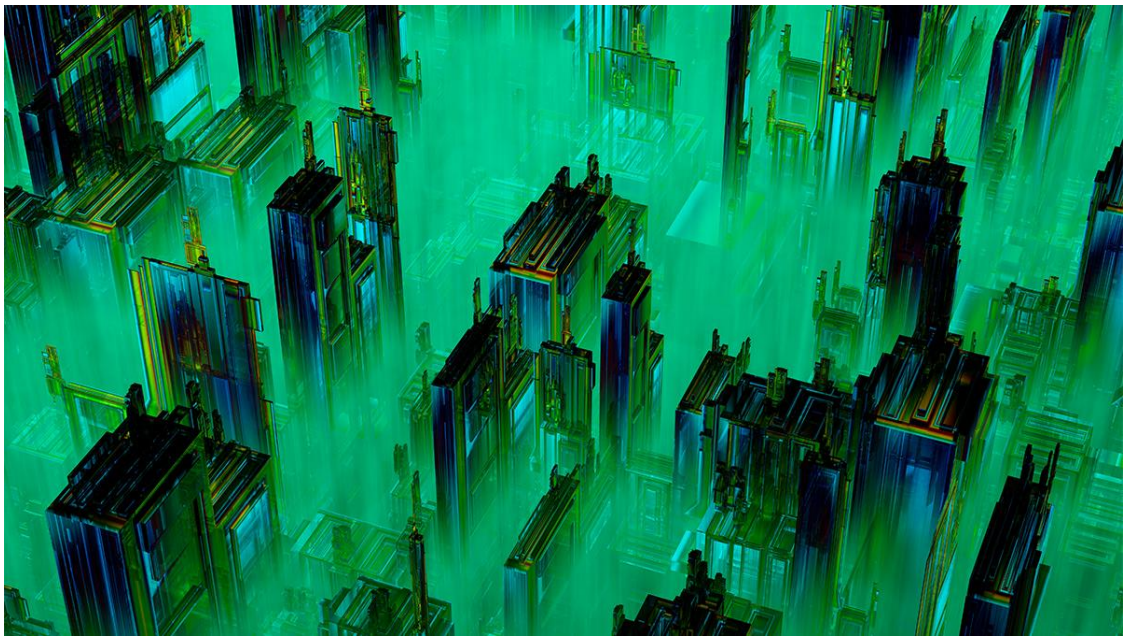
Harvard Business Review

Cybersecurity And Digital Privacy

What Russia's Ongoing Cyberattacks in Ukraine Suggest About the Future of Cyber Warfare

by Stuart Madnick

March 07, 2022



Westend61/Getty Images

Summary.

For years, Ukraine has been a proving ground Russian for cyber weapons. As companies and countries watch the latest chapter of the Russian war in Ukraine unfold, they should take heed of the conflict's online front — and think about how to prepare if (and more likely when) it spills over Ukraine's borders. While some attacks, such as those on infrastructure, are nearly impossible for companies to prepare for, there are steps that they should take as a matter of course: make sure software is up to date and patched, check that you have effective and up-to-date malware and antivirus software, and ensure that all important data is backed up in a safe location.

Between 1946 and 1958, the Bikini Atoll, in the North Pacific Ocean, was used as a testing ground for 23 new nuclear devices that were detonated at various spots on, above, or beneath it. The point of the tests was primarily to understand (and, in many cases, show off) how these new weapons really worked — and what they were capable of. The era of nuclear testing may now be over, but the age of cyber warfare is just beginning. And for Russia, the war with Ukraine has been likely serving as a live testing ground for its next generation of cyber weapons.

Countries and companies watching this latest chapter unfold should remember this: The online front of the war can — and has — jumped borders.

Unlike conventional attacks, cyberattacks can be hard to accurately attribute. Plausible deniability exists because in many cases, cyberattacks can be launched from an unwitting host. For example, partial control of your home computer could be taken over, without you knowing it and used to initiate a chain of attacks. One such event occurred in 2013 when smart refrigerators were made part of a botnet and used to attack businesses. In 2016, many thousands of home security cameras were taken over and used to disrupt the operations of Twitter, Amazon, Spotify, Netflix and many others.

But there's strong evidence tying Russian hackers to a string of attacks in Ukraine. Going back to 2015, after the Russian invasion of the Crimean Peninsula, suspected Russian hackers managed to knock out electric power for around 230,000 customers in western Ukraine. Attackers repeated the trick the following year, expanding the list of targets to include government agencies and the banking system. In the hours before Russian troops invaded, Ukraine was hit by never-before-seen malware designed to wipe data — an attack the Ukrainian government said was "on a completely different level" from previous attacks.

It's easy to understand why Ukraine is an appealing target for testing cyberwar capabilities. The country has similar infrastructure to that found in Western Europe and North America. But unlike the United States, the United Kingdom, and the European Union (EU), Ukraine has more limited

resources to counter-attack (though the U.S. and EU have both provided support in bolstering its cyber defenses). And while Russia is the obvious suspect, it's certainly possible that other countries, such as Iran, North Korea, or China, have been testing their own cyber weaponry in Ukraine, too.

The larger point here is that there's little chance that cyberattacks will be limited to Ukraine. Governments and corporations should closely heed what's going on there, because cyberwar can — and has — quickly spread across borders.

What might a real global cyberwar look like

Given that the U.S. and EU have banded together in support of Ukraine, the scope of a cyberwar could be broad. Large scale cyber skirmishes can become global due to a spillover effect. There's some precedent for what a spillover would look like. In 2017, a suspected Russian attack featuring a piece of malware dubbed "NotPetya" disrupted Ukrainian airports, railways, and banks. But, NotPetya did not to stay in Ukraine. It spread rapidly around the world, infecting — and for a period of time largely shut down — a diverse array of multinational companies including the global shipping company Maersk, the pharmaceutical giant Merck, FedEx's European subsidiary TNT Express, and among others.

In my research with colleagues, and investigations by others, we've observed that most cyberattacks have not been as devastating as they could have been. It might be because the attacker was not fully aware of how much damage could have been done but, maybe more likely, these were just "tests" of the cyberweapons. As our research has shown, it is not only possible to cause systems such as electric grids to shut down, but also to cause them to explode or self-destruct — damage that could take weeks or longer to repair. There have so far been few such attacks, but in some cases, steel mills and gas pipelines have been destroyed. Probably the best known case was the Stuxnet cyberattack which is believed to have destroyed some 1,000 centrifuges in an Iranian uranium enrichment facility.

So, what might a real, global cyberwar look like? Given the interdependence of critical infrastructure sectors, such as electricity and communications, an aggressive attack would likely knock down many sectors at the same time, magnifying the impact. Furthermore, in a "no holds barred" attack where maximum damage was inflicted, a primary goal would be to also produce long-lasting physical damage.

The two kinds of cyberattacks

I often note two different impacts of cyberattacks: direct and indirect.

Indirect attacks: By indirect, I mean neither you nor your computer are individually targeted. The target would be the power grid, supply chains, banking systems, water treatment, communications, and transportation. There is not much you can do personally to defend these systems. But, how well, and how long, can you fare without electricity, food, water, and cash?

Direct attacks: By direct, I mean an attack targeting you. In war, the civilian population, either deliberately or accidentally, can also be targeted to weaken the desire to continue the war. In cyberwarfare the technical methods are quite similar, but the consequences can be more personal. For example, what if all the data on your computer is stolen or erased, especially if those are the only copies of photos or documents.

So what can you do to protect yourself?

Indirect cyberattack: You personally may have no way to protect the nation's critical infrastructure. But, by collectively influencing the government, the private sector can be motivated to improve its protection, preparation, and, maybe even more important, improve its resilience in the face of such breaches.

Many may not realize that many types of cyberattacks are not required to be reported. As a result, the government and other similar companies have no idea that cyberattacks — attempted as well as actual — are going on. For example, pipeline companies were not required to report cyberattacks until *after* the publicity of the Colonial Pipeline attack. I believe the "bad guys" do a much better job of sharing information than their targets, who

may have an interest in keeping quiet about an attack. That needs to change if we are to be better informed and prepared.

Regarding resilience of our infrastructure, we often don't realize how badly prepared we are until too late. A serious cyberattack can have a similar impact to a natural disaster, knocking out essential infrastructure and creating cascading crises. It could, for example, resemble the 2021 winter freeze in Texas caused massive disruptions, loss of electricity, and over 200 deaths. And it could have been much worse. The Texas Tribune reported that the "Texas' power grid was 'seconds and minutes' away from a catastrophic failure that could have left Texans in the dark for months."

There's also the collateral damage. In the case of the Texas freeze, as reported by the Insurance Council of Texas, a nonprofit trade association, "the number of claims due to frozen and burst pipes will be unlike any event the state has experienced." Even the water pressure in some cities was significantly reduced due to the water flowing from these burst pipes. Many electricity generating stations temporarily had to be stopped due to load unbalances, but then were unable to restart. That was because many of the "last-resort power units," basically the starter motors for the plants, did not work, likely because they had not been tested. That is like finding out that the batteries in your flashlights are dead only *after* your electric power has gone off.

Companies should push for assurances that our infrastructure can rapidly recover *after* a cyberattack *before the cyberattack*, and have those assurances verified by independent auditors.

Direct cyberattack: Most of the key things that you can do to prevent, or at least minimize, direct damage to you and your computer fall under the "Cyber Hygiene 101" category. This includes simple measures, such as having a strong password and not clicking on suspicious links — precautions many of us unfortunately overlook. But, we now know that there are ways to get onto your computer, such as Solarwinds, Log4j, and Pegasus, without you doing anything and which don't require your password. These are called "zero click vulnerabilities."

As such, preparing for a cyberattack means doing everything possible to minimize potential damage if the attacker does get in. This includes:

- Making sure that your software is up-to-date throughout your organization, and that known vulnerabilities in earlier versions have been patched.
- Having effective antivirus and malware detection software — and remember, malware may already be laying dormant on your computer, awaiting orders.
- Frequently backing up your important data, such as documents that are only stored in once place, in case it is destroyed.

It's also worth taking steps in your organization to minimize risk and prepare to respond if (or when) the worst happens. This includes:

- Looking for possible vulnerabilities in your cyber supply chain, and pushing vendors of third-party software to prioritize cybersecurity.
- Testing your incident response plan — including running scenarios and tabletop exercises — to be sure that the plan is sound and that everyone knows what they're supposed to do in a crisis.

There was a time, in the 1960's and 1970's, when the world feared a global nuclear war. Fortunately, we made it through that period. With luck, we will also avoid a devastating global cyber war. But there is no guarantee and with geopolitical tensions rising to high levels, it is not wise to just rely upon good luck. Each of us needs to do everything that we can to increase the chances of being a survivor.

Acknowledgement: This research was supported, in part, by funds from the members of the Cybersecurity at MIT Sloan (CAMS) consortium.

Stuart Madnick is the John Norris Maguire (1960) Professor of Information Technologies in the MIT Sloan School of Management, Professor of Engineering Systems in the MIT School of Engineering, and Director of Cybersecurity at MIT Sloan (CAMS): the Interdisciplinary Consortium for Improving Critical Infrastructure Cybersecurity. He has been active in the cybersecurity field since co-authoring the book *Computer Security* in 1979.