The Washington Post
Democracy Dies in Darkness

Some see cyberwar in Ukraine. Others see just thwarted attacks.

By Joseph Marks with research by Aaron Schaffer

April 14, 2022 at 7:23 a.m. EDT

Welcome to The Cybersecurity 202! Here's a great poem from former U.S. poet laureate **Robert Hass** about April in my hometown. (For what it's worth, I never encountered half those woodland animals when I lived there). We're off Friday but will be back in your inbox Monday.

Below: Russia may be behind dangerous new malicious software that could cause explosions at energy plants, and Microsoft disrupted a band of zombie computers called ZLoader.

Cyber fizzle or cyber bang in Ukraine? Experts are divided.

As Russia's Ukraine invasion grinds through its second month, **experts are still divided over whether hacking is playing a meaningful role in the conflict.**

As the fog of the initial invasion clears, some argue that cyberattacks are a critical component – reversing earlier assessments that the invasion had been surprisingly light on hacking.

The evidence: Attacks include satellite hacks that interfered with Ukrainian communications during the early days of the invasion and a recently thwarted electricity sector hack that could have shut off power for 2 million people. Ukrainians have also blamed Russia for deploying malicious software to wipe data from government and industry computers.

"This is full-on, full-scale cyberwar," Microsoft vice president of customer security **Tom Burt** said in a Wall Street Journal interview.

Other cyber analysts, however, still say hacking has basically been a sideshow – one that has had little if any significant impact on the outcome of a conflict that has been overwhelmingly defined by deadly Russian airstrikes and other conventional military operations.

"The[re's] a lot of cyber fizzle, but not a lot of cyber bang," **Jacquelyn Schneider**, a researcher at Stanford University's Hoover Institution focused on technology and national security, told me.

“Cyber operations can't win wars. And they don't start wars either. But they make wars harder to fight and they drain manpower, resources, and time,” she told me.

Two lenses

Why such widely divergent interpretations of the same basic set of facts? One reason is broader assumptions about a field that’s both relatively new and notoriously murky.

- Some analysts view cyber events in Ukraine so far as a harbinger of far more damaging hacks to come.
- Others say they’re a sign that the most damaging hacks take more effort than it’s worth during a shooting war – even for a cyber superpower like Russia.

A recent Foreign Affairs article made the first case.

“A full accounting of the cyber-operations reveals the proactive and persistent use of cyberattacks to support Russian military objectives,” the authors, NATO officials **David Cattler** and **Daniel Black**, wrote. “The misperception that Russia has been restrained or ineffective in the prosecution of its cyberwar on Ukraine likely stems from … an unrealistic test of strategic value.”

They go on to warn that “Russian President Vladimir Putin is most likely to double down on early cyber-successes and seek to further disrupt and undermine government, military, and civilian infrastructure, as well as defense industrial base enterprises.”

CATO Institute Senior Fellow **Brandon Valeriano** is a skeptic. In Valeriano’s view, Kremlin cyber operations in Ukraine since the invasion have just been a logical extension of hacking Russia has been doing there for several years and largely unrelated to broader military strategy.

Even the most damaging cyberattacks – such as a 2015 Russian attack that disrupted large portions of Ukraine’s energy grid for several hours – would be impractical during wartime because the same effect could be achieved more easily with missiles.

“A lot of people have their hopes pinned on this new evolution of warfare and that’s not something that’s come to pass in Ukraine,” he told me.

However: Even if cyberattacks aren’t the most damaging part of a war, they still could play a bigger role than they have in Ukraine so far.

“War is always going to be about killing people and destroying things. Cyber operations can complement that … but it’s not going to win a large-scale war and it’s never going to [be] the story of the war,” **Jon Bateman**, a Cyber Policy Initiative fellow at the Carnegie Endowment for International Peace and a former Pentagon cybersecurity official, told me.

Looking ahead

Cyber warfare could play a far more decisive role in future conflicts – especially if the hacking victim has put less effort into its cyber defense than Ukraine, which has invested substantially in cyber protections since Russia’s 2014 invasion of Crimea.

The United States and other Western nations have also made extensive efforts to help Ukraine combat cyber threats. And Russia has also underperformed in nearly every aspect of the invasion – cyber included.

Consider Estonia: Russia's 2007 cyberattacks against Estonia, for example, were highly successful, in part, because they blocked Estonian media and made it tough for leaders to get accurate information out to citizens. Estonia has become a highly capable cyber player since then.

If Russia had succeeded in blocking Ukrainian President Volodymyr Zelensky from rallying his people and the rest of the globe online that might have swayed the course of the conflict, noted **Suzanne Spaulding**, an Obama administration cyber official who's now a senior adviser at the Center for Strategic and International Studies.

"We might have been lucky," Spaulding told me. "I'm not ready to say this is evidence that cyber can't really impact a conflict."

The keys

New malware could cause explosions in energy plants, authorities say

Officials from the Cybersecurity and Infrastructure Security Agency (CISA) and other agencies didn't say what country developed the software, which was discovered before it was used, Joseph Menn reports.

But industry experts who worked with government agencies to analyze the malware said it was probably Russian, that its top target was probably liquefied natural gas production facilities, and that it would take months or years to develop strong defenses against it.

"This is going to take years to recover from," said **Segrio Caltagirone**, vice president of threat intelligence at Dragos and a former global technical lead at the National Security Agency.

The U.S. government is encouraging the energy sector and other industries to install monitoring programs and take security steps such as requiring authentication beyond a password to access company networks.

Microsoft disrupted an army of zombie computers used for hacking

A court authorized Microsoft to take control of domains used by a gang of cybercriminals to "grow, control and communicate with" the army of infected devices known as a botnet, the company said. The botnet dubbed ZLoader infected more than 200,000 devices in businesses, homes, hospitals and schools, Microsoft said.

Botnets are used for a variety of hacking activities. ZLoader was also used to deliver ransomware to victims.

- In all, ZLoader has targeted more than 100 banks, e-commerce sites and other organizations, a Microsoft researcher said in a court filing.

- Microsoft also accused Crimean Peninsula resident **Denis Malikov** of being a perpetrator "behind the creation of a component used in the ZLoader botnet to distribute ransomware"

Microsoft credited several companies and other organizations with assisting the botnet disruption, including ESET, Lumen's Black Lotus Labs, Palo Alto Networks Unit 42, the Financial Services Information Sharing and Analysis Centers, the Health Information Sharing and Analysis Center and Avast.

Russian regulator monitored online dissent, leaked documents indicate

The regulator known as Roskomnadzor monitored social media, blogs and other Internet postings to identify "hotbeds of tension" and shared reports with the Russian government about "the destabilization of Russian society," the Latvia-based Russian news site Meduza reports.

Information about the programs came from documents published by Distributed Denial of Secrets. The transparency collective's source for the documents "urgently felt the Russian people should have access to information about their government" and "also expressed their opposition to the Russian people being cut off from independent media and the outside world," the group wrote.

National security watch

Op ed outlines the best U.S. response to a Russian cyberattack

If Russia hits the United States in cyberspace, U.S. officials should respond with tailored cyberattacks aimed at increasing economic pressure on the Kremlin while limiting civilian damage, Silverado Policy Accelerator founder **Dmitri Alperovitch** and RAND Senior Political Analyst **Samuel Charap** write in a Post op ed this morning.

One option would be an attack that creates a brief but widespread disruption to Russian internet service, they write.

"It would be beneficial for the United States to tailor a response that can provide a powerful demonstration to the Kremlin of U.S. capabilities but avoid widespread destruction that could lead to escalation," the pair write. "Combined with a clear public and private message that the United States will go much further in the cyber arena if Russia attacks again, such a move would demonstrate America's resolve while creating an off-ramp for Moscow to end its cyber aggression."

Industry report

Industry groups lay out requests for Biden's forthcoming identity theft executive order

The groups want the Biden administration to:

- Accelerate state deployment of mobile driver's licenses, including through grants, so people can better prove their identities online.

- Mandate the creation of a government-wide system for verifying information that would be "accessed with uniform fees and terms by the public and private sector."
- Direct the Commerce Department's National Institute of Standards and Technology to work on a Digital Identity Framework so government agencies can follow standards promoting security, privacy and interoperability.

The priorities were laid out in a letter to top Biden administration officials signed by the Better Identity Coalition, Cybersecurity Coalition, Electronic Transactions Association, Identity Theft Resource Center, National Cyber Security Alliance and the U.S. Chamber of Commerce Technology Engagement Center.

Neurodiverse candidates find niche in remote cybersecurity jobs (Wall Street Journal)

Government scan

U.S. pushes U.N. to cut N.Korea oil imports, ban tobacco, blacklist Lazarus hackers (Reuters)

DHS investigators say they foiled cyberattack on undersea Internet cable in Hawaii (CyberScoop)

Cyber insecurity

After a brief decline, organizations once again are bombarded with ransomware (The Record)

Chat room

NATO's cyber defense center is welcoming Ukraine into its ranks. While Ukraine isn't a NATO member, the NATO-affiliated center invited Ukraine to participate in its work during the early phases of the Russian invasion.

Daybook

- CIA Director **William J. Burns** speaks at the Georgia Institute of Technology today at 11 a.m.
- Wayne Law's Voting Rights and Election Law Society and the Levin Center at Wayne Law host an event on best practices for election audits today at 12:15 p.m.
- The Joint Service Academy Cybersecurity Summit kicks off at 10:30 a.m. on April 20.

Secure log off

"And as for my experience of myself, it comes and goes, I'm not sure it's any one thing, as my experience of these creatures is not." Thanks for reading. See you tomorrow.