The New York Times

The Ukrainian Cyberwar That Wasn't

March 11, 2022
Farhad Manjoo

Late last year, the United States and Britain sent experts to Ukraine to help its government prepare for the spectacular cyberattack that some believed would be Vladimir Putin's opening salvo during an invasion. Ukraine's electricity grid was said to be a particularly attractive target for Russian hackers, who managed to shut it down for brief periods twice before.

The next attack, many worried, could be altogether more devastating. Under Putin, Russia has adopted a form of fighting that marries conventional military force with unconventional, often digital operations, like online political propaganda and cyberattacks on infrastructure. For years, security officials in the West have worried about Russia's hacking capabilities; Western military planners routinely hold elaborate war games to prepare for a damaging surprise attack by Russia (or, other times, China) — what the former defense secretary Leon Panetta once called a coming "cyber-Pearl Harbor."

"I don't think there's a slightest doubt that if there is an invasion or other kind of incursion into Ukraine, it will start with cyber," Angus King, the independent senator from Maine, told The Times in December.

But something cyberunexpected happened on the way to cyberarmageddon: Russia invaded Ukraine the old-fashioned way, with tanks and guns and missiles and airplanes, and there was little evidence that it accomplished anything meaningful with weapons of code. There were reports of an uptick in attacks on Ukrainian websites in the months leading up to war, but their impact has been minimal. Two weeks into the fighting, Ukraine's electricity grid, its communications systems and other infrastructure are still largely up. Its president is streaming from his government office.

"Despite being one of the world's foremost offensive cyberpowers, the Russian invasion of Ukraine has, thus far, been utterly conventional in its brutality," Ciaran Martin, a former cybersecurity official for the British government, wrote last week in Lawfare.

What accounts for Russia's apparent cyberrestraint? Nobody quite knows. Russia could be holding back its best cyberweapons for a more critical time in the war. It could also just be incompetent. Maybe its hackers were no match for Ukraine's cyberdefenses, which the country has been beefing up for years.

But the relative quiet on the Ukrainian cyberfront has some cyberexperts suggesting something unusual: That perhaps the national security establishment's picture of digital attacks as a unique

and revolutionary new front in warfare has been off the mark. That's not to say that cyberattacks aren't a serious threat; they are costly and could conceivably cause great chaos and even bodily harm. As offensive weapons of war, though, they may have been oversold. Cyberweapons face severe limitations, and there is a growing body of research suggesting that they frequently fail to achieve battlefield goals.

"It's not magic," Brandon Valeriano, a senior fellow at the Cato Institute who studies cyberweaponry, told me. "It's not transformational. It's not going to change the character of war."

Among other problems, cyberweapons are difficult to target and control. Because computer networks are connected to other computer networks, a viral hack aimed at Ukraine might escape into its NATO neighbors, forcing a wider conflict that Russia might want to avoid. Cyberweapons are also by nature slow and difficult to rely on. Hackers may need to spend months studying an enemy's infrastructure in order to attack it, but the attack can fall apart in an instant if the enemy discovers an intrusion.

Considering these limitations, a cyber-Pearl Harbor or cyber-9/11 is the wrong metaphor for understanding these systems, Valeriano and other researchers say. Rather than battlefield-defining attacks, cyberweapons are better suited as weapons of espionage, sabotage and other covert operations. Like the cane or pen gun from the James Bond movies, they make for a neat spy trick but are unlikely to alter the international order the way aircraft carriers, precision-guided munitions or nuclear weapons have.

Some have seen a more revolutionary role for them. In "The Perfect Weapon," his 2018 book on the rise of cyberweapons, the Times reporter David Sanger argued that these weapons are unusual because they are very cheap, very stealthy and, unlike other novel weapon systems, available to a wide range of powers, from poor, isolated rogue nations like North Korea to former superpowers like Russia to criminal gangs and terrorist groups.

Lucas Kello, an associate professor of international relations at Oxford who is a leading proponent of the idea that cyberweapons might be groundbreaking, has suggested that they could be as transformational for the international order this century as nuclear weapons were last century. He argues that cyberweapons will alter the world order by creating a state of relations between nations that he calls "unpeace" — a status somewhere between all-out war and complete peace, in which nations attack one another digitally in ways that produce major damage but don't escalate to physical conflict.

These predictions are troubling, but they haven't yet been proved in battlefield conditions. The political scientists Nadiya Kostyuk and Yuri M. Zhukov studied how cyberweapons have been used in Ukraine and Syria. In both cases, they wrote in a 2017 paper, "cyberactivities failed to compel discernible changes in battlefield behavior."

Perhaps the fundamental reason for their failure, as Thomas Rid argued in his 2013 book "Cyber War Will Not Take Place," is that cyberattacks are not inherently acts of war. Cyberattacks are rarely violent. They are rarely instrumental. While they may damage or annoy an enemy, they

don’t often cause hardships that push an enemy toward a specific goal. And they are not always political. In many cases, perhaps the majority, cyberattacks are better suited to criminal or intelligence ends (stealing money, gaining information) than to shifting political calculus. In that sense, Rid said, cyberattacks are not weapons of war like nuclear bombs but are instead “sophisticated acts of network-enabled sabotage, espionage and subversion.”

This, of course, is great. It should be cause for celebration that cyberweapons aren’t the second coming of nuclear weapons. But for some theorists, there is a sadness to this realization, too, because it suggests that war will continue to be as physically brutal as it’s always been.
“A lot of people get this great idea that war is going to be very digital, and it’s not,” Valeriano told me. “The whole function of war is an abhorrent practice in human society. And technology is not going to sanitize that.”