Zyri

The non-existent Ukrainian cyber war

Farhad Manjoo

March 14, 2022

Late last year, the United States and the United Kingdom sent experts to Ukraine to help its government prepare for the spectacular **cyber attack** which some believed would be the initial attack of **Vladimir Putin** during an invasion.

The Ukrainian power grid was said to be a very attractive target for Russian hackers, who had already managed to shut it down for short periods on two previous occasions.

Many feared that the next attack would be much more devastating.

The Annonymous cyberattack on Russian TV channels. Explosion in the Ukraine inserted in the French subsidiary of RT.

Under Putin, Russia has adopted a way of fighting that combines conventional military force with unconventional, often digital, operations such as online political propaganda and cyber-attacks on infrastructure.

For years, security officials in the West have worried about Russia's hacking ability; Western military planners frequently play elaborate war games in order to prepare for a **Surprise attack** harmful by Russia (or, at other times, China), which the former Secretary of Defense **Leon Panetta** once called the next **"Pearl Harbor cibernético".**

"I don't think there is the slightest doubt that if there is an invasion or any other type of incursion into Ukraine, it will be cyber first," Maine Independent Senator Angus King told T**he New York Times** in December.

Yet something happened **cyber-expected** on the road to cyberarmageddon:

Russia invaded Ukraine the old-fashioned way, with tanks, guns, missiles and planes, and there was little evidence that it achieved anything significant with source weapons.

There were reports of an increase in attacks on Ukrainian websites in the months leading up to the war, but their impact has been minimal.

Two weeks after the fighting, Ukraine's power grid, communication systems and other infrastructure are still generally functional.

The President of Ukraine continues to broadcast from his government office.

"Despite being one of the world's leading offensive cyber powers, the Russian invasion of Ukraine has, so far, been one of utterly conventional brutality," Ciaran Martin, a former British government cybersecurity official, wrote last week in Lawfare.

What is the reason for **apparent containment** Russian cyber?

Nobody knows for sure.

Russia may be saving its best cyber weapons for a more critical moment in the war. It's also possible that it's just **incompetent.**

Perhaps his hackers were no match for Ukraine's cyber defenses, which the country has been beefing up for years.

But the relative calm on the Ukrainian cyber front has some cyber experts suggesting something unusual:

that perhaps the image that national security agencies have of digital attacks as a new revolutionary united front in warfare is incorrect.

This is not to say that cyber attacks are not a serious threat; They are **expensive** and could cause great chaos and even physical damage.

However, as offensive weapons of war, they may have been overrated.

Cyber weapons face serious **limitations**and a growing body of research suggests they often fail to achieve their intended objectives on the battlefield.

"They're not magic," Brandon Valeriano, a senior researcher at the Cato Institute who studies cyber weaponry, told me.

"They are not transformative. They are not going to change the character of the war."

Among other problems, cyber weapons are difficult to command and control.

Because computer networks are connected to other computer networks, a viral hack targeting Ukraine could slip through to its NATO neighbors, forcing a **wider conflict** that Russia might want to avoid.

Also, by nature, these weapons are slow and unreliable.

Hackers may need to spend months studying the enemy's infrastructure in order to attack it, but the attack can collapse in an instant if the enemy discovers the intrusion.

Given these limitations, a Pearl Harbor or cyber 9/11 is the wrong metaphor for understanding these systems, Valeriano and other researchers say.

Rather than battlefield-defining attacks, these types of weapons are more appropriate as instruments of espionage, sabotage, and other covert operations.

Just like the cane or the pen in the movies **James Bond**are a good espionage trick, but unlikely to disrupt international order the way aircraft carriers, precision munitions, or nuclear weapons have.

There are those who consider that these weapons can have a more revolutionary role.

In "The Perfect Weapon," his 2018 book on the rise of cyber weapons, Times reporter **David Sanger** He argued that these weapons are unusual because they are so cheap, so stealthy, and

unlike other novel weapons systems, they are available to a wide range of powers, from corrupt, poor, and isolated nations like North Korea to former superpowers like Russia. through criminal organizations and terrorist groups.

Lucas Kello, Associate Professor of International Relations at the **Oxford University** and one of the main proponents of the idea that cyber weapons can be revolutionary has suggested that they could be as transformative for the international order in this century as nuclear weapons were in the last century.

He maintains that this type of weapons will alter the world order creating a state of relations between nations that he calls "**not of peace**", an intermediate state between declared war and total peace, in which nations attack each other digitally in a way that causes significant damage, but without reaching physical conflict.

These predictions are worrying, but they have yet to be tested on the battlefield.

Political scientists Nadiya Kostyuk and Yuri M. Zhukov studied how these weapons have been used**as in Ukraine and Syria.**

In both cases, they wrote in a 2017 article, "cyber activities failed to force 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 cyber attacks are not intrinsic acts of war; they are seldom violent and seldom decisive.

Although they can damage or annoy an enemy, they do not usually cause difficulties that lead the enemy to a specific target.

And they are not always political.

In many, perhaps most, cases, cyberattacks are better suited for criminal or intelligence purposes (stealing money, obtaining information) than changing political calculus.

Rid asserts that, in this sense, cyberattacks are not weapons of war like nuclear bombs, but are "sophisticated acts of **sabotage,** espionage and subversion that use the network".

Of course this is good news.

It should be cause for celebration that cyber weapons are not the next version of nuclear weapons.

But for some theorists this is also sad to realize because it suggests that the war will continue to be as violent as ever.

"Many think that the war is going to be very digital, and it is not like that," Valeriano told me.

"The function of war is to be an abhorrent practice in human society, and technology is not going to make amends for that."