THE NATIONAL INTEREST

# Paper Tigers: Proxy Actors Are the True Cyber Threats

**By focusing on the mythical power of the great nations, the cyber community risks missing the true threats to digital order.**

by Brandon Valeriano, Jose Macias

April 12, 2022

As the war in Ukraine evolves, a perplexing question remains: why did the world not witness the hybrid warfare projected in Russian doctrine? And further, as the United States has supplied weapons to Ukraine and waged economic warfare against Russia, why hasn't Putin fought back against the United States in cyberspace? These questions go to the heart of Russia's capabilities and intentions. Revealing itself to be the paper tiger it has always been, Russia continues to demonstrate its inability to achieve operational success in Ukraine. The latest such event is Russia's failure to disrupt the Ukrainian power grid a month after the war began. There is a clear disconnect between Russia's actual abilities and its willingness to wreak havoc, particularly when compared to the dramatic predictions before the war. It is essential to adopt a forward-looking strategy that looks beyond Russia and focuses on the actors that would be willing and able to cause cyber havoc.

From Israel supporting the NSO Group to the United Arab Emirates employing former NSA hackers and, more recently, the rise of the Ukrainian "IT Army," the states and proxy actors with the capabilities to cause real destruction are sometimes those that we least expect. These are the often-overlooked actors with the will and intent to cause harm.

Long ago, Harvey Starr and Ben Most articulated the conditions of opportunity and willingness in conflict. Many states have the opportunity to launch a war, but the willingness to engage in combat is dictated by a complex set of calculations. Like traditional conflicts, both factors are necessary conditions for cyberwar. Historically, the cybersecurity community has failed in its evaluation of willingness or intent, with a whole host of predictions never coming true, a "Cyber Pearl Harbor" most prominent among them.

Cybersecurity analysts often fail to explain motivation and action in the international system because their focus is typically on technological processes. It is the unexpected actors and proxies that tend to trigger war, and the true surprises come from examining past patterns and extrapolating from them, as counterintuitive outcomes often defy predictions based on the imagination. From Serbia setting off a powder keg in twentieth-century Europe to Ukraine and Iraq being perceived as key threats to great powers, it has always been the unexpected third party that draws states into war. Almost all wars with more than two parties involve a minor party dragging the other sides into the fight. On the other hand, it is rare for dyadic interstate conflicts to trigger a devastating major power confrontation.

### The Big Five and Proxy Actors

Most accounts of cyberwar focus on what is called the "big five": Russia, China, North Korea, Iran, and the United States. These are certainly the most active states in the cyber domain, but are they the most dangerous? As we enter a new era of cyberwar, expectations need to be managed and threat inflation must be avoided. As John Arquilla has argued before, there is a form of mutually assured destruction in cyberspace that can limit violence. If both sides are vulnerable in similar ways, they will shift their focus to arenas where they have an advantage.

The true danger of cyber proxy actors is that they are not limited by the norms that constrain most states. While limited in their capabilities and ability to coordinate, actors like the teenage hacking group Lapsus$ demonstrate the potential devastation that independent actors can cause in cyberspace. Third-party proxy actors like the Ukrainian IT Army, Anonymous, and the Syrian Electronic Army tend to be willing to cause harm, but they often lack the bureaucracy, networks, and tools that make state actors so effective.

The Russo-Ukrainian war is a tragedy, but it is also a prime opportunity for Ukraine to showcase and hone its newly created IT Army. The Ukrainian IT Army is entirely justified in its actions; Ukraine has been invaded, with incredible devastation left in the wake of Russia's retreat from Kyiv. Russia has cut off all international and independent news, making cyber actions prudent ways of causing domestic pain to Russia. Recently, the IT Army caused chaos in Russia by leaking the emails of active Russian soldiers, hacking electrical charging stations, and exposing the food delivery orders of the Russian FSB. Not exactly the grand cyberwar we were all promised, but disruptive nonetheless.

Critically, the United States and its NATO allies must avoid getting caught in the crossfire, a likely scenario if actions by the independent Ukrainian IT Army get confused with actions directed by the United States or NATO. Accidents risk leading to escalation, and the biggest fear is the possibility of Russia misperceiving Ukrainian proxy actions in cyberspace.

Overall, Russia is weakened and will be focused on developing a stalemate with Ukraine for a generation. At the same time, China is focused on espionage, both for innovation and control over its domestic population. Iran is concentrated on regional actors, using proxies to attack Saudi Arabia and Israel. Moreover, Tehran is using ransomware tactics and taking lessons from the North Koreans to buttress its isolated regime. Finally, North Korea is certainly a belligerent actor, but its cyber soldiers are looking for cryptocurrency while the leadership focuses on making videos displaying their new missiles.

## The True Threats

It is the unrestrained and unfocused actors that are the true threats in the cyber domain. These are the actors that would sell their capabilities to other states or operate from the shadows as proxy actors with little accountability.

A key threat vector is repression. Take, for instance, the Israeli NSO Group, which operates with engagement from the Israeli government. As a reminder, the U.S. Department of Commerce placed the NSO Group on a "trade blacklist" after it was found to have supplied malware to foreign governments. The goal is repression—targeting dissidents, protestors, and other activists like Jamal Khashoggi. NSO's links to other governments are extensive, with a recent report finding that Mubadala Capital, part of a fund chaired by Abu Dhabi crown prince Sheikh Mohammed bin Zayed al-Nahyan, provided capital for NSO.

Of course, cyber threats differ across countries. But with a few outliers, the cyber community devotes very little time to African threat actors. And as China receives the lion's share of attention, the dynamics of other Asian cyber actors are also often ignored. Things are even worse in the case of Latin American cyber threats. The cyber potential of cartels as proxy actors is ignored; no one asks what will happen when capos decide to save ammunition and invest in developing digital tools for their fight against the Mexican government. Cartels have mastered money laundering and won hearts and minds through donations, but what if they launch a propaganda machine using information warfare tactics, machine learning, and natural language processing?

The simple fact is that expectations are often quite different than the future reality. By focusing on the major states—the big five cyber powers being the usual suspects—cybersecurity scholars and policymakers will remain blind to the true challenges to global order. While it is state-sponsored threats today, the cyber-powered cartels in Latin America, state-funded cyber firms in the Middle East, and netizens of East Asia will be the true concerns tomorrow. By focusing on the mythical power of the great nations, the cyber community risks missing the true threats to digital order: the small, unrestrained actors who have little to lose and a lot to gain.

*Brandon Valeriano is a Senior Fellow at the Cato Institute and a Distinguished Senior Fellow at the Marine Corps University and the Krulak Center.*

*Jose Macias is a Public Policy Fellow with the Congressional Hispanic Caucus Institute placed at the Center for Strategic and International Studies.*