

THE WASHINGTON POST – 3 MARZO 2025

## **U.S. digital disarmament gives Russia free rein in cyberspace. Bad idea**

*di Colin Ahern e Mark Montgomery*

*Colin Ahern is New York State chief cyber officer. Mark Montgomery is a retired rear admiral and senior director of the Center on Cyber and Technology Innovation at the Foundation for Defense of Democracies.*

On the heels of the stunning Oval Office meeting between President Donald Trump and Ukrainian President Volodymyr Zelensky comes the news of a shocking — and shockingly misguided — reversal of long-standing U.S. national security policy regarding Russian cyber operations.

In an alleged bid to bring Russian President Vladimir Putin to the negotiating table, the Trump administration has reportedly [ordered](#) both the Defense Department's Cyber Command and the Department of Homeland Security's Cybersecurity and Infrastructure Security Agency [to stand down](#) from monitoring and countering Russian cyberthreats.

Having spent more than five decades combined defending America's national interest and digital infrastructure, we unequivocally maintain that this policy shift is a strategic error that will make the United States less secure in cyberspace while doing little to bring about peace in Europe.

Although the administration asserts the stand-down is only a pause during negotiations, it is nevertheless an ill-advised approach that violates two fundamental principles of international relations and cybersecurity.

First: Negotiations with adversaries proceed best from a position of strength, not weakness. By unilaterally disarming — even temporarily — in the digital domain, we

sacrifice our leverage and invite further aggression, not concessions. The administration appears to believe that by extending an olive branch to Moscow, we will be rewarded with reciprocal restraint. History suggests otherwise, and Trump's [first national security memorandum](#) says the same. Putin respects strength and exploits perceived weakness, including with extrajudicial killings abroad.

Second, the administration fundamentally misunderstands the global strategic landscape. While it apparently hopes to separate Russia from the “axis of aggressors” (China, Iran and North Korea), Moscow has shown no interest in distancing itself from these partners. Just days ago, Sergei Shoigu, secretary of Russia's Security Council, [met with Chinese President Xi Jinping](#) in Beijing to reaffirm their “deep partnership.” Russia gains far more from aligning with these powers than from any concessions Washington might offer. And unilaterally standing down key offensive and defensive U.S. capabilities means we have fewer options to bring Putin to the table, not more.

This is not a partisan issue — both [Republicans](#) and [Democrats](#) have long recognized the dangers of American weakness in the face of our adversaries and the specific vulnerabilities the United States faces in defending its cyberspace. Putin's disastrous war of choice in Ukraine can seem far away, but the Trump administration's actions should be reappraised quickly. Not doing so will put American economic and national security at grave risk here at home.

The scale of this reported retreat in cyberspace is significant. Suspending all cyber operations planning against Russia — including offensive digital actions and preparations — and limiting our efforts to look for malicious Russian cyber activity in our cyberspace is nonsensical.

There has been extensive [reporting](#) of Chinese “Volt Typhoon” efforts to penetrate U.S. critical infrastructures in preparation for later disruption or destruction. Russia is an equally sophisticated and persistent cyber adversary. Every day, Russian-backed hackers target American hospitals, businesses and schools, with [canceled classes](#) harming our children, [hospitals diverting ambulances](#), [blood supplies being](#)

[placed at risk](#) and businesses [paying millions of dollars](#) in ransoms to cyber terrorists. As one government insider put it bluntly: “[Putin is on the inside now.](#)”

The Trump administration owes the American people an accounting of how it is planning to keep U.S. critical infrastructures safe from a determined adversary. To cease planning offensive operations is to prepare for defeat. To stop monitoring Russian cyber activity is to deliberately blind ourselves to imminent threats. The country needs the Departments of Defense and Homeland Security to do *more* against Russian cyber aggression, not less.

The administration’s defenders might argue that this policy shift reflects a new strategic calculation or a grand bargain with Moscow. But what concessions have we secured in return? Has Russia agreed to rein in ransomware gangs operating from its territory? Has it pledged to stop targeting our critical infrastructure? Have we received any verifiable commitments whatsoever? There can be no trade-off or deal: There is only support for a dictator attacking Americans and retreat from our sacred obligations to defend our country. These moves put Putin — not America — first.

The uncomfortable truth is that we are unilaterally surrendering a critical domain of national power while apparently receiving nothing in return. If Trump wants a breakthrough with Russia, now is the time to double down on using all elements of American power, not to prematurely capitulate. The administration should immediately reverse this dangerous policy before the damage becomes irreparable. In cyberspace, as in all domains, peace comes through strength, not surrender.