THE NATIONAL INTEREST

How Cyber Restraint Makes Us All Safer

Avoiding cyber doom takes the dedicated work of a restrained power.

Brandon Valeriano

May 2, 2022

At a broad, strategic level, restraint emphasizes doing less with less; protecting a narrow set of core interests in ways that respect the limits of power. In cyberspace, restraint pushes back against the inevitability of an offensively dominated "cyberwar" and seeks to avoid spirals of escalation and threat inflation.

Cyber restraint seeks to reduce the impact of digital harm through preventative measures such as target hardening and resilience to improve defense and foster stability. Restraint hopes to avoid the offensive cyber operations that are likely to spiral and harm civilians. Rather, focusing on building internal capacity, improving international communication, and creating more domestic and international defensive partnerships will allow the United States to avoid triggering the disasters often predicted in cyberspace and ensure its own stability.

Why Cyber Restraint?

Logically, it is difficult to push for anything but restraint in cyberspace. Cyberspace is simply not built for warfare despite decades of warnings from pundits about the danger of "Cyber Pearl Harbors" that typically describe large-scale attacks with wide-ranging and devastating impacts.

Despite predictions of doom, reality has played out differently. States cannot help but be restrained in cyberspace due to the vulnerability of all aspects of society to digital attack. Cyber operations are not typically coercive—meaning they do not change a target's behavior—however, critical aspects of society, including industrial control systems for daily necessities like water and power, are still vulnerable to disruption.

Dramatic cyberattacks that shock and awe the target have not been borne out through either empirical observations or doctrine. Russia's evident cyber restraint during its 2022 invasion of Ukraine should make U.S. policymakers reconsider the impact of cyber operations during war. Instead of unleashing offensive operations in coordination with the invasion, Russia only launched operations that sought to disrupt and spy on the adversary. Digital destruction is not a replacement for conventional weapons.

U.S. cyber strategy has previously been characterized by restraint, but over time it has moved toward more aggressive doctrines. The central proposition of a strategy of cyber restraint is that

digital operations are not expanding the range of possible harm. A proper focus on resiliency and target hardening forestalls most forms of digital disaster.

Current U.S. cyber strategy draws a direct line between going on the offense and forcing positive changes in the target's behavior, but there is no evidence that cyber operations can coerce. By emphasizing offensive operations Washington invites retaliation and escalation, the opposite of strategic stability. Breaking the norms against aggression only creates new norms of offensive action that will harm the United States.

A layered strategy is critical to creating order; there is no single line of action, and each policy requires simultaneous implementation to achieve effective results. The first layer should create conditions in the international system for the enfranchisement of positive norms and rules that ensure collaborative behavior for all who use cyber operations as a part of national policy. Establishing international norms of behavior help create stable expectations and ensure order, but it is important to mold and reinforce these norms.

The United States should issue a declaratory cyber strategy to establish stable expectations. Moving forward, U.S. cyber strategy must have clearly defined limits of behavior. Vaguely stating the need to respond is insufficient compared to clearly stating what happens when lines are crossed. The imposition of costs can be achieved through actions such as diplomacy, sanctioning, and degrading capabilities by sharing malicious code to warn the international community.

The final layer is defense enabled through target hardening. After failing for over a decade to take the defense seriously, positive moves are finally establishing core defenses. Hardening the target involves enabling the Cyberspace and Infrastructure Security Agency (CISA) as part of the Department of Homeland Security (DHS). Working with the FBI, CISA can be the first point of contact for U.S. domestic actors attacked in cyberspace. Without the defense done right, the entire house of cards collapses in on itself.

Cyber Restraint in Reality

A strategy of cyber restraint offers a positive vision for the future. By focusing on core foundations including shaping the international environment, establishing the limits of action, and providing support for the defense, cyber security can move beyond simple strategies that do not connect reality to policy. The United States and global community can and should do better.

A layered defensive strategy focused on creating stable norms, declaring the limits of cyber action, and the foundations of defense articulate a positive, restrained vision for cyber security into the future. Properly evaluating the threat, meeting the challenge, and finding methods of minimizing damage will all ensure that the continuity of the government and society will be the prime goal of strategy. Avoiding cyber doom takes the dedicated work of a restrained power.

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