INSTITUTE FOR DEFENSE ANALYSES

Persist in Cyber Initiative or Lose

Michael P. Fischerkeller, Project Leader
Emily O. Goldman
Richard J. Harknett

May 2022

IDA NS D-33120

INSTITUTE FOR DEFENSE ANALYSES
730 East Glebe Road
Alexandria, Virginia 22305

The Institute for Defense Analyses is a nonprofit corporation that operates three Federally Funded Research and Development Centers. Its mission is to answer the most challenging U.S. security and science policy questions with objective analysis, leveraging extraordinary scientific, technical, and analytic expertise.

About This Publication

This work was conducted by the IDA Systems and Analyses Center under contract HQ0034-19-D-0001, Project C5224, "Review and Editorial Prep for Non-sponsored Articles and Essays for External Publication," for the IDA. The views, opinions, and findings should not be construed as representing the official position of either the Department of Defense or the sponsoring organization.

Acknowledgements

For More Information

Michael P. Fischerkeller, Project Leader
mfischer@ida.org, 703-845-6784

Margaret E. Myers, Director, Information Technology and Systems Division
mmyers@ida.org, 703-578-2782

Copyright Notice

Rigorous Analysis | Trusted Expertise | Service to the Nation

Persist in Cyber Initiative or Lose

Michael P. Fischerkeller, Emily O. Goldman, and Richard J. Harknett

The United States can lose its relative power position in the world today without losing an armed conflict. This is because cyberspace has opened a new avenue for international competition that co-exists alongside the more familiar nuclear and conventional strategic environments where states interact in militarized crisis and war. Competition in and through cyberspace, short of threat or use of force, has become potentially as strategically consequential for relative gain and loss as war and militarized crisis have been throughout history.

The strategic logic driving cyberspace campaigns, operations, and activities, however, is distinct from that which we associate with the nuclear and conventional environments and, thus, with militarized crisis and armed conflict. It calls for operating continuously in and through cyberspace, seizing opportunities to advance national interests in competition while setting favorable conditions for potential crisis and conflict. It rests on anticipating the exploitation of one's own vulnerabilities while leveraging the capacity to exploit others' vulnerabilities. Because of the fluidity of digital technology and its uses, security rests on seizing and sustaining the initiative in this exploitation dynamic. If one can sustain the cyber initiative, it becomes possible to achieve strategic success either by inhibiting the consequential gains of your opponent or by achieving such gains for yourself.

By 2018, the United States began to align its military cyberspace operations to this cyber strategic logic with a new operational approach—persistent engagement—along with new authorities and policies that enable initiative persistence. As we argue in a new book, *Cyber Persistence Theory: Rethinking National Security in Cyberspace,* initiative persistence is essential to reducing cyber insecurity. Some U.S. allies are also instituting changes aligned with this logic. Russia, China, North Korea, and Iran have been operating with initiative persistence for years, seizing opportunities and exploiting vulnerabilities for cumulative gain while eroding U.S. power. Strategic intent reflects relative global position. Accordingly, Russia, China, North Korea, and Iran are operating in and through cyberspace to grow their power, circumvent obstacles, and undermine their adversaries, while the U.S. and its allies are operating to preserve the current (and, from their perspective, favorable) status quo.

States need not align with the logic of strategic environments, and even when they do, success is not assured. Opponents might simply be better at competing and contesting. But if states do *not* align to the structural imperatives of strategic environments, they most certainly will lose. The incontestable behavioral fact of continuous action in cyberspace wherein states persistently exploit cyber and cyber-enabled vulnerabilities for advantage is a telling shift away from the security logics demanded by the other strategic environments. In the nuclear environment, security derives from the absence of action and the threat to respond. In the conventional environment, security depends on episodic action in militarized crisis and armed conflict. The difference in successful pathways to advancing positive national security outcomes between the nuclear, conventional, and cyber strategic environments could not be starker.

It is important to recognize the implications of these differences for achieving national security. Since the cyber strategic environment incentivizes states to continuously act, the metric for success of persistent engagement as an operational approach, as well as a broader cyber security strategy aligned with the environment, is not altering an adversary's decision calculus to act. Security rests on inhibiting

continuous adversarial cyber competitive activity to a point where its effects are not strategically impactful. The goal of initiative persistence is to preclude strategic consequences, not shape mindsets.

Adversaries Were the First to Recognize and Act

For at least a decade, the United States emphasized the development of exquisite cyber capabilities and accesses to support an off-the-shelf threat of response in what the Department of Defense (DoD) Cyber Strategy of 2015 enshrined as a "doctrine of restraint." This approach fell comfortably within the expectations drawn from Cold War nuclear threat success in deterring strategic action—war—from occurring. The clear metric of success was the absence of a significant cyber incident—that is, a strategic armed-attack equivalent cyber action.

However, none of the United States' main adversaries were operating from the same logic. Cyber capabilities were being employed continuously through operations and campaigns in a seemingly experimental approach with lessons learned informing iterative advancements in further cyber action. U.S. restraint coincided with adversary adventurism and U.S strategic losses. Many in U.S. policy and academic circles blamed this adversarial cyber activity on the failure of getting deterrence correct, rather than seeing it for what it represented—the recognition by U.S. adversaries of a new strategic environment in which strategic gains could be realized from continuous activity below the threshold at which deterrence functions effectively.

The Democratic People's Republic of Korea (DPRK) learned that it could circumvent extraordinary international sanctions through cyber exploitation and manipulation of financial infrastructure and transactions. The DPRK's cyber campaign funded nuclear weapons and ballistic missile development programs that sanctions were trying to prevent, such as the recently deployed ballistic missile that can target most locations in the continental United States. Should its programs continue apace, U.S. Northern Command assesses that the DPRK will be able to overwhelm the U.S. Ground-Based Midcourse Defense System by 2025.

China's cyber campaigns targeting the intellectual property (IP) of the U.S. defense industrial base (DIB), U.S. technology companies, and other forward-leaning growth sectors have been growing in scope, scale, and sophistication. Illicit acquisition of IP from the DIB has allowed China to threaten, and in some cases erode, U.S. overmatch through accelerated and truncated research and development. IP theft coupled with an ability to rapidly re-innovate it into indigenous products has helped China stave off a slowdown in economic growth. Left unabated, such cumulative gains will lead to sustained U.S. relative power loss.

Russia's well-documented cyber activity focuses not on circumventing or competing but on continuously stress-testing democratic institutions and alliances with the goal of undermining the essential trust that is required for the United States to operate as a great power. Left uncontested, trust in democracy will erode.

Adversaries are employing cyber means to achieve specific strategic objectives tied directly to their respective positions in the distribution of global power relative to the United States.

The U.S. Experience with Initiative Persistence

Persistent engagement has begun to take root in U.S. strategy. Early critics' concerns that adopting a continuous cyber operational tempo would undermine U.S support for international "norms" and/or escalate into crisis or armed conflict have not materialized. Moreover, adoption of persistent engagement is producing effects unimaginable just a few years ago when current operational principles, authorities, and capabilities were not in place. These include a new Presidential policy delegating more authorities to the DoD for cyberspace operations below the use of force and cyber-specific statutory provisions that clarified the status of military cyber operations as traditional military activities exempt from covert action approval and oversight procedures.

Persistent engagement prescribes that the United States defend forward both geographically (beyond DoD networks) and temporally (ahead of adversary exploitation) thereby enabling anticipatory resilience in domestic and foreign partner networks. Cyber National Mission Force Commander General Joe Hartman explains, "We get to find our adversaries in foreign space before they're able to come to America and compromise our network. And while we do that, we get to make our partners and allies safer." Timely security successes include disrupting Russian interference in the 2018 and 2020 elections and degrading Trickbot malware infrastructure.

Initiative persistence is equally relevant to other U.S. Government agencies that possess cyber operational capabilities and authorities to act. Consider the Federal Bureau of Investigation's (FBI) Rule 41 of the Federal Rules of Criminal Procedure. Prior to 2018, the FBI leveraged Rule 41 in reaction to the Kelihos botnet. FBI redirected Kelihos-infected computers to a substitute server that recorded their Internet Protocol addresses so the government could provide victim's addresses to Internet service providers (and others) who could help remove the malware. Since 2018, Rule 41 has been leveraged to support proactive anticipatory operations that protect compromised U.S. companies' networks, systems, and devices before adversaries can act. The FBI removed the Webshell installed by China's Hafnium advanced persistent threat (APT) from hundreds of servers and removed the CyclopsBlink command and control (C2) malware associated with a Russian APT from thousands of devices. In the latter operation, the FBI also closed the external management ports being exploited to access the C2 malware.

There are other examples of initiative persistence. Working together and with a third party, the FBI and U.S. Cyber Command disrupted REvil ransomware operations. Both organizations have released information on adversary techniques, tactics, and procedures, as well as indicators of compromise through VirusTotal and Cybersecurity and Infrastructure Security Agency (CISA) alerts to inoculate U.S. companies from malicious cyber actors. Collaboration with the private sector to get ahead of cyber attacks has matured under U. S. Cyber Command's Under Advisement program and CISA's Joint Cyber Defense Collaborative.

Persistent engagement in competition applies not only to countering malicious cyber actors; it can be employed to contest ill-gotten adversary gains from non-cyber activities and to set conditions to support deterrence in militarized crisis and victory in war. When asked about the importance of persistent engagement in the context of the Russia-Ukraine armed conflict, U.S. Secretary of Defense Lloyd Austin stated that persistent engagement "is absolutely critical" and is paying dividends for Ukraine while also providing the U.S. and its allies with early warning when a developing threat is identified. Amy Zegart has accurately described the relentless and pro-active U.S. intelligence disclosure campaign to control the Russia-Ukraine narrative as a form of persistent engagement that seizes and maintains the narrative initiative, at least for Western audiences.

The *Financial Times of London* reported on a U.S. Cyber Command hunt forward mission in December 2021 where members of the Cyber National Mission Force worked alongside Ukrainian network operators to discover and mitigate a wiper malware capable of disrupting rail networks across the country. Millions of Ukrainians took to the railway system to escape the Russian assault on their cities. This may be the first reported cyber activity that directly saved lives. Some speculate that Russia's initial plan was to place intense pressure on the Kyiv government to cause a quick collapse. Did that plan rest on a strategic assumption that civilians would be trapped in cities because the rail system would not function, thus inducing intense pressure and potential panic? If historians find this to be the case, we may look back on this hunt forward operation as having had a strategic impact in the conduct of a conventional war.

Other examples of initiative persistence in the shadow of conflict have come to the fore. A few hours before the Russian invasion, Microsoft detected new malware—FoxBlade—intended to disrupt Ukraine's digital infrastructure. On the U.S. government's advice, Microsoft immediately extended the warning to neighboring NATO countries. Ukraine's cyber operators, for their part, shared with the U.S. (and others) the discovery of a novel industrial control system malware (Industroyer2).

Moments of fundamental change in how national security must be achieved are rare. But when they do occur, failure to adjust correctly and effectively can mean the difference between growing as a great power or being pushed off of the pedestal and withering. Persistent engagement is the correct adjustment to the reality of cyber insecurity. The critical next steps are to scale it up while maintaining tempo and to build it out into a cornerstone of a whole-of-nation-plus (WON+) cyber framework. Initiative persistence in managing the potential exploitation of network vulnerabilities must drive inter-agency coordination and action, public-private alignment of interests and action, and individual citizen engagement and action. All three elements must also align with international partners' orientations and actions (i.e., the "+" in WON+). In an environment of continual action in the setting and resetting of network structures, processes, and components, the stark choice is to persist or lose. The good news is that the United States, as a status quo defensively oriented state, is figuring this out and beginning to regain some initiative in cyberspace by leading through action to cultivate norms of responsible behavior and set the terms for stabilizing cyber activity globally. The strategic stakes in moving forward on this course cannot be overstated.

REPORT DOCUMENTATION PAGE

Form Approved
OMB No. 0704-0188

1. REPORT DATE (DD-MM-YY)	2. REPORT TYPE	3. DATES COVERED (From – To)
00-05-22	Non-Standard	

4. TITLE AND SUBTITLE	5a. CONTRACT NUMBER
Persist in Cyber Initiative or Lose	HQ0034-19-D-0001
	5b. GRANT NUMBER
	5c. PROGRAM ELEMENT NUMBERS

6. AUTHOR(S)	5d. PROJECT NUMBER
Michael P. Fischerkeller, Emily O. Goldman, Richard J. Harknett	C5224
	5e. TASK NUMBER
	5f. WORK UNIT NUMBER

7. PERFORMING ORGANIZATION NAME(S) AND ADDRESSES	8. PERFORMING ORGANIZATION REPORT NUMBER
Institute for Defense Analyses 730 East Glebe Road Alexandria, VA 22305	NS D-33120

9. SPONSORING / MONITORING AGENCY NAME(S) AND ADDRESS(ES)	10. SPONSOR'S / MONITOR'S ACRONYM
Institute for Defense Analyses 730 East Glebe Road, Alexandria, VA 22305	IDA
	11. SPONSOR'S / MONITOR'S REPORT NUMBER(S)

12. DISTRIBUTION / AVAILABILITY STATEMENT

Approved for public release; distribution is unlimited.

13. SUPPLEMENTARY NOTES

Project Leader: Michael P. Fischerkeller

14. ABSTRACT

The United States can lose its relative power position in the world today without losing an armed conflict. This is because cyberspace has opened a new avenue for international competition that co-exists alongside the more familiar nuclear and conventional strategic environments where states interact in militarized crisis and war. Competition in and through cyberspace, short of threat or use of force, has become as potentially strategically consequential for relative gain and loss as war and militarized crisis have been throughout history.

15. SUBJECT TERMS

Cyberspace, cyber strategy, persistent engagement

16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT	18. NUMBER OF PAGES	19a. NAME OF RESPONSIBLE PERSON
a. REPORT	b. ABSTRACT	c. THIS PAGE			Institute for Defense Analyses
Unclassified	Unclassified	Unclassified	Unlimited	4	19b. TELEPHONE NUMBER (Include Area Code)