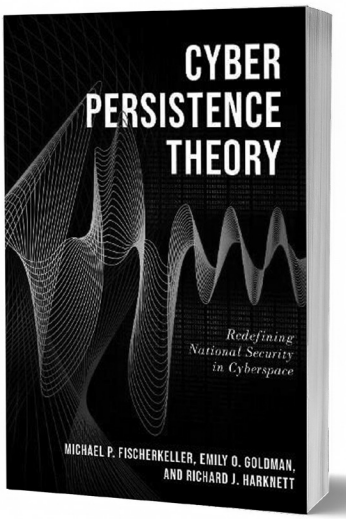
Cyber Persistence Theory: Redefining National Security in Cyberspace

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

Reviewed by
Dr. Mark Grzegorzewski



EXECUTIVE SUMMARY

Cyber Persistence Theory provides an important discussion of the structural shift in cyber strategy necessary for taking U.S. cybersecurity to the next level. No other work has made such a convincing case for this structural shift as the authors explain the current gap between cyber theory and observed cyber application. This alternative to the cyber deterrence paradigm provides an in-depth, academic analysis of the modern cyberspace environment. The main takeaway of this thesis is that cyberspace activity, especially exploitation, is the primarily form of strategic competition, and that exploitation should be interpreted as an alternative to war wherein states quickly capitalize on other state's cyberspace vulnerabilities rather than resorting to compellence. According to the authors, in cyberspace, states operate, at a low-cost, out of a structural need to persist and a strategic incentive to achieve short-term gains, without necessarily triggering an armed attack.

The book also emphasizes that the nature of cyberspace diminishes international cooperation, leading to a state of constant competition between countries. This structural feature, according to the authors, should encourage us to view cyberspace differently from the nuclear realm, while also emphasizing that strategic gains accumulate

Dr. Mark Grzegorzewski is an assistant professor of cybersecurity at Embry-Riddle Aeronautical University in the Security Studies and International Affairs Department. He is also an Army Cyber Institute Fellow. His recent publications include: "911? We Have an Emergency: Cyberattacks on Emergency Response Systems," "In Search of Security: Understanding the Motives Behind Iran's Cyber-Enabled Influence Campaigns," and "Why the United States Must Win the Artificial Intelligence (AI) Race," Dr. Grzegorzewski worked for over 11 years in the Department of Defense, seven of those years for U.S. Special Operations Command. He holds a Ph.D., M.A., and B.A. in Political Science/Government from the University of South Florida and a graduate certificate in Globalization Studies.

over time via successful tactical operations within campaigns. This suggests that by effectively conducting cyber operations, a state can enhance its relative power without resorting to traditional warfare.

REVIEW

Martin Libicki's "Cyberspace in Peace and War" (2nd edition) seminal work has been a must-read for anyone trying to understand the cyber domain and deterrence. However, in *Cyber Persistence Theory,* Fischerkeller, Goldman, and Harknett identify that, in practice, Libicki's cyber deterrence formulation seems to be an imperfect fit for the future cyber strategic environment. In hindsight, the authors identify the cause of this mismatch as being obvious and rather simple: The U.S. government has been applying a 60-year-old nuclear deterrence paradigm to a completely unique strategic domain, cyberspace. In *Cyber Persistence Theory: Redefining National Security in Cyberspace*, the authors propose a new strategic concept for cyberspace that aligns closely with USCYBERCOM's strategy of "Persistent Engagement."

This alignment with USCYBERCOM's strategy of "Persistent Engagement" is no coincidence, as the authors' book serves as its unambiguous intellectual underpinning of the 2018 strategic-level strategy, which all had a hand in formulating. The authors possess impeccable credentials. Each of them has experience in strategy, cyber, and strategic studies. Fischerkeller is an Institute for Defense Analyses (IDA) researcher who has spent over 20 years supporting the Department of Defense (DoD). Goldman led the team that wrote the 2018 USCYBERCOM vision and currently serves as a USCYBERCOM strategist. And Harknett is the Director of the School of Public and International Affairs, Co-Director of the Ohio Cyber Range Institute, and Chair of the Center for Cyber Strategy and Policy

at the University of Cincinnati and was the inaugural USCYBERCOM Scholar-in-Residence. These authors' experiences complement each other well and add more to this compelling thesis together than either could do alone.

The book's initial focus is on this mismatch between cyber strategy and operations by examining previous literature, explaining how we got into our current predicament: We were too successful with our nuclear deterrence strategy. As the authors note, this presents a dilemma. Cyber strategy thinkers are boxed in by what they know and what was successful in the past. This causes cyber strategists to be anchored to the past, even though the old paradigm no longer quite fits and the old measures of success are no longer relevant. The authors conclude that in such circumstances, we must look for alternatives. In response to this imperfect fit, we've seen a new cyber paradigm emerge, at least within USCYBERCOM, "Persistent Engagement."

In developing the reasoning for the new persistent engagement paradigm, the authors advance the claim that there are three strategic domains, conventional, nuclear, and cyber, and that cyber is a domain of exploitation, unlike the conventional domain of conflict and the nuclear domain of coercion. As the authors assert, these three domains each have unique defining features. The conventional domain uses fighting and winning in war to achieve security conditioned by conflict. The nuclear domain uses the absence of war conditioned by offense dominance merely from the threat of use and a resulting no-win situation. The cyber domain presents an alternative, leading to war conditioned by competition.

In making this argument, the authors argue that the cyber strategic environment is novel since it is characterized by a dominant technology which poses unique challenges to international security. They further assert that the cyber domain has core exceptional features which make it mutable, interconnected, and macro-resilient while at the same time micro vulnerable, due to an abundance of cyberspace vulnerabilities. Moreover, the constant contact is a permanent condition of cyberspace since all instruments of national power can engage other states and these states can engage right back due to the compression of space and time. The result is that in cyberspace, states are engaging each other constantly. This is in contrast to the conventional domain, where states also engage, yet their experience is episodic and characterized by having to cross physical space, or the nuclear domain whether the engagement tends to be more psychological by way of deterrence to have the intended effect.

The authors reason that in cyberspace, states are distinct entities like in the physical world, yet in the virtual domain states engage each other irrespective of physical geography. This condition impacts how states view their perception of security in cyberspace. The authors argue that states must persist in this virtual domain and achieve dominance by relentlessly engaging and taking advantage of adversaries' cyberspace vulnerabilities, while seeking to protect their own cyber networks, critical infrastructure, and national prerogatives as best

they can. In cyberspace, a vulnerability that is there one day, may be patched and closed-off the next. This is precisely why states must persistently engage and exploit opportunities in cyberspace. Clearly, the conceptualization of security in cyberspace is very different than that in the conventional domain.

To support these assertions, the authors employ the international relations concept of *fait accompli*. In cyberspace, a *fait accompli* is understood as a limited unilateral gain at a target's expense, where that gain is retained when the target chooses to relent rather than escalate in retaliation. The 2020 Russian Solar Winds hack provides such an example. The hack was treated, primarily, as an act of espionage, rather than an act of war, and the U.S. did not overtly respond in-kind to the Russian operation. The authors posit, this is often due to states learning about the intrusion long after it occurs. The logic is that since they have no recourse to get back what was stolen, they then have little incentive to respond long after the fact. While states could respond long after the fact, such actions could send a misguided signal to the adversary, thereby furthering misperceptions between the states and possibly destabilizing the environment. As a result, states often accept that a breach occurred and that a cyber incident impacted their information systems, and they reason that the intrusion likely does not warrant a response. As the authors note, ultimately by states not reacting to these incidents and thus accepting that adversary cyber exploitation will occur against them, they signal a tacit understanding and acceptance between states regarding cyberspace operations and activities.

In pressing this argument, *Cyber Persistence Theory* highlights that the world largely has not seen Russia, China, Iran, and North Korea holding targets at risk to destroy or disable in the event of hostilities, but rather taking advantage of cyberspace vulnerabilities they can exploit. An example is China's cyber economic espionage over the past 20 years. Individually, these actions might not appear connected, but taken as a whole, are indicative of a state-led campaign leading to strategic effects (i.e., growing Chinese economic dominance and diminishing American power). The authors assert these campaigns can achieve aims similar to war and can often lead to other strategic outcomes such as achieving economic aims. This description presents cyber as an "alternative to war" and highlights why the offense-defense rubric for cyberspace operations makes little sense in today's parlance and is unhelpful for discussions about cyber strategy.

Having laid the preparatory groundwork, the authors press the argument in support of their thesis. Cyber stability comes from the structure of the cyber domain that includes guardrails to constrain state behavior. These guardrails come in the form of tacit coordination and tacit bargaining. Tacit coordination arises when parties with common strategic interests align their actions implicitly without direct communication. Tacit bargaining involves informal agreements reached through actions and patterns, allowing both sides to perceive

and establish boundaries based on observed behaviors, fostering clarity, predictability, and stability. Ultimately, tacit coordination and bargaining produces mutually dependent actions, and regularity, in the cyberspace.

Given these theoretical underpinnings, cyber persistence theory was applied to the United States as a case study. The authors reiterate that the peace-war dichotomy did not work in cyberspace, and demonstrate that the moment a country pauses, they cede the operational initiative. An important outcome is that when this occurs, countries no longer hold targets at risk but rather are left to look for opportunities to what exploit cyber network insecurities when they find them. These instances demonstrated that the world was witnessing was not war, nor was it coercion. A new phenomenon had emerged that U.S cyber strategy could not conceptually capture. This phenomenon reflected that adversarial countries were competing differently than the United States in cyberspace.

Realizing around 2013 that the Cold War nuclear deterrence paradigm had been misapplied and the "doctrine of restraint" had allowed offenders to operate without the consequence in U.S. networks, the United States needed a new approach. With this realization, the United States bought into the development of persistent engagement strategy in the cyber domain. The 2018 "defend forward" cyber strategy aimed to re-align U.S. cyber strategy with the cyber environment and provided the foundations for this new strategy. This strategy contains four pillars: (1) Defend the homeland by protecting networks, systems, functions, and data; (2) Promote American prosperity by nurturing a secure, thriving digital economy and fostering strong domestic innovation; (3) Preserve peace and security by strengthening the ability of the United States—in concert with allies and partners—to deter and, if necessary, punish those who use cyber tools for malicious purposes; and (4) Expand American influence abroad to extend the key tenets of an open, interoperable, reliable, and secure Internet. These pillars, particularly 1 and 4, incorporate aspects of persistent engagement, provide an alternative to the deterrence paradigm, and provide an alternative to war in achieving strategic outcomes.

CONCLUSION

Cyber Persistence Theory makes an important contribution to and provides highly reasoned basis for understanding the evolution of U.S. cybersecurity strategy to "persistent engagement." The lack of applicability of the deterrence paradigm to cyberspace was an open secret, and this work is an order of magnitude towards properly re-conceptualizing cyberspace operations in strategic studies. Using the familiar lexicon of international relations, this work both describes a more apt theory and prescribes a strategy that better aligns with the realities of cyberspace than traditional cyber deterrence.

While the authors properly note that cyberspace is primarily a space of exploitation, they leave open the possibility that it could deter in limited circumstances, in cases such as holding critical infrastructure at risk. They also note that there's a distinct secondary behavior observed, primarily among certain non-state actors. For instance, hacktivist groups often use distributed denial of service or DDOS attacks on government websites, aiming to coerce rather than merely exploit. For those actors, cyber deterrence is still an effective strategy, but it does not mean it cannot be complemented by cyber persistence.

Indeed, today, we still observe both strategies in play. Yet, as we navigate new strategic alternatives in cyberspace, there's an inherent reluctance to abandon previously effective strategies. Eventually, this profound paradigm shift will impact how we approach global cyber security.

Full citation (as seen in this CDR Book Review):

Title:	***Cyber Persistence Theory: Redefining National Security in Cyberspace***
Authors:	Michael P. Fischerkeller, Emily O. Goldman, and Richard J. Harknett
Publisher:	Oxford University Press
Paperback:	272 Pages
Price:	$20.99 Paperback
	$13.79 Kindle