The US Army War College Quarterly: Parameters

Volume 50
Number 3 *Parameters Autumn 2020*

Article 9

8-14-2020

A Bizarre Pair: Counterinsurgency Lessons for Cyber Conflict

Jason Healey

Recommended Citation
Jason Healey, "A Bizarre Pair: Counterinsurgency Lessons for Cyber Conflict," *Parameters* 50, no. 3 (2020), doi:10.55540/0031-1723.2676.

Technological Innovation

A Bizarre Pair: Counterinsurgency Lessons for Cyber Conflict

Jason Healey

ABSTRACT: The lessons of counterinsurgency have deeper implications for cyber conflict than previous research has identified. Two decades of experience in Iraq and Afghanistan provide insights into the cyber strategy of defending forward including treating major cybersecurity and technology companies as host-nation partners and focusing on winning the hearts and minds of global netizens.

Existing research has yielded significant insights into cyber capabilities as effective means for irregular warfare, but little research has been devoted to applying lessons from irregular warfare and counterinsurgency to winning cyber conflict. This does not mean there is a direct and deep equivalence, only that some of the mindset and culture for successful counterinsurgency can be useful for cyber warriors. For example, major cybersecurity and technology companies are, in important ways, analogous to host nations in cyberspace with unique capabilities the US military cannot replicate. Sometimes more firepower and applying overmatch wins. Sometimes—especially when civilians and civilian infrastructure cannot be separated away from battle, as in counterinsurgency and cyber—these efforts can make the problem worse. And sometimes there is no military path to victory. Ultimately, the United States may have to choose between taking the fight to the enemy and winning the support of America's, and indeed the globe's, netizens.

After nearly 20 years of combat in Iraq and Afghanistan, the US military has learned hard lessons about fighting irregular warfare and counterinsurgency, but the relevance of these lessons to cyber conflict and competition have been overlooked. Though the details differ, current US cyber strategy is rooted in thinking similar to that on conventional fights in the land, sea, or air. "We must take this fight to the enemy, just as we do in other aspects of conflict," noted General Paul Nakasone, the commander of US Cyber Command.[1] The new DoD strategy for winning in cyberspace and an associated US Cyber Command vision emphasize the lethality of US offensive capabilities, taking action to "defend forward" and "disrupt or halt malicious cyber activity at its source."[2] The overall goals are to achieve "overmatch" and "achieve

Jason Healey, senior research scholar and adjunct faculty at Columbia University's School for International and Public Affairs, is the editor of *A Fierce Domain: Conflict in Cyberspace, 1986 to 2012.*

[1] Paul M. Nakasone, "A Cyber Force for Persistent Operations," *Joint Force Quarterly* 92 (1st Quarter 2019): 11, https://ndupress.ndu.edu/Media/News/News-Article-View/Article/1736950/a-cyber-force-for-persistent-operations/.

[2] United States Department of Defense (DoD), *Summary: Department of Defense Cyber Strategy* (Washington, DC: DoD, September 2018), 1.

and maintain superiority in the cyberspace domain."[3] "A good offense," summarized the Chairman of the Joint Chiefs of Staff, General Mark Milley, "is critical and that is the best defense."[4]

The sustained application of initiative, maneuver, and firepower would not have seemed out of place to General Ulysses S. Grant. "The art of war is simple enough. Find out where your enemy is. Get at him as soon as you can. Strike him as hard as you can and as often as you can, and keep moving on."[5] But Iraq and Afghanistan proved warfare is not always as straightforward as Grant supposed. The dynamics of irregular warfare and counterinsurgency can be a distorted mirror image of those of the traditional battlefield.

Offensive Capabilities and Irregular Warfare

The Department of Defense defines irregular warfare as: "a violent struggle among state and nonstate actors for legitimacy and influence over the relevant populations. Irregular warfare favors indirect and asymmetric approaches, though it may employ the full range of military and other capabilities, in order to erode an adversary's power, influence, and will."[6] For additional clarity, the Department further focuses on threat actors who use irregular means "such as guerrilla warfare, terrorism, sabotage, subversion, criminal activities, and insurgency."[7]

Cyber capabilities have long been framed as especially useful as a means for such irregular warfare, a topic which featured heavily in some of the earliest research, including that of Winn Schwartau, Dorothy Denning, John Arquilla, and others. More recent research, especially at institutions of higher military learning, have examined issues like developing an "unconventional cyber warfare employment methodology" and exploring ideas like "cloud-powered foreign internal defense" and "counternetwork COIN."[8]

The unique characteristics of cyber capabilities make them relatively easy to fold into operations across the range of irregular warfare. The most obvious examples might be cyberattacks intended to take down Ukraine's electrical grid, the disruption of US elections, and sabotage of

[3] US Cyber Command (USCYBERCOM), *Achieve and Maintain Cyberspace Superiority: Command Vision for US Cyber Command* (Fort Meade, MD: USCYBERCOM, April 2018), 4–5.

[4] *Nomination—Milley: Hearing before the United States Senate Committee on Armed Services*, 116th Cong. (July 11, 2019) (statement of General Mark A. Milley), https://www.armed-services.senate.gov/hearings/19-07-11-nomination_--milley.

[5] Eric Foner and Olivia Mahoney, *A House Divided, America in the Age of Lincoln* (New York: W. W. Norton & Company, 2018), 113.

[6] Office of the Joint Chiefs of Staff (JCS), *Irregular Warfare: Countering Irregular Threats Joint Operating Concept*, vers. 2.0 (Washington, DC: JCS, May 17, 2010), 9, https://www.jcs.mil/Portals/36/Documents/Doctrine/concepts/joc_iw_v2.pdf?ver=2017-12-28-162021-510.

[7] JCS, *Irregular Warfare*, 9.

[8] Christopher R. Eidman and Gregory Scott Green, "Unconventional Cyber Warfare: Cyber Opportunities in Unconventional Warfare" (master's thesis, Naval Postgraduate School, 2014), 3; and Patrick Michael Duggan, "Strategic Development of Special Warfare in Cyberspace," *Joint Force Quarterly* 79 (4th Quarter, 2015): 49–50, https://ndupress.ndu.edu/Media/News/Article/621123/strategic-development-of-special-warfare-in-cyberspace/.

the production of weapons of mass destruction.[9] Other examples include intelligence agencies orchestrating bank and cryptocurrency heists for hundreds of millions of dollars, hacking a television station and blaming Islamic State terrorists, or using state assets to attack private companies.[10] Cyber capabilities are useful to state actors. "Nobody wants full-on war. . . . It's bad for business. Irregular warfare tactics give these states a degree of plausible deniability and nominally push the responsibility of escalation off of their shoulders."[11]

Lessons for Cyber from Counterinsurgency

Unlike research on cyber as a tool for irregular warfare, far less research has been devoted to understanding how irregular warfare might inform cyber strategies. In 2011, Greg Rattray and I analyzed how lessons from irregular warfare can apply to cyber, which was subsequently addressed by another scholar.[12] In 2012, we applied findings from research on counterinsurgency, irregular warfare, and stability and recovery operations to cyber conflict.[13] More recently, practitioners summarized the major past trends in research utilizing the Counterinsurgency Diamond Model (analyzing the population, disruptors, controllers, and governance) and proposed several strategies.[14] Another recent piece examined the failure to apply lessons

[9] Adrian Bonenberger, "Ukrainian Elder Statesman: How Russian Hybrid War Is Changing the World Order," *Foreign Policy*, March 21, 2017, https://foreignpolicy.com/2017/03/21/ukrainian-elder-statesman-how-russian-hybrid-war-is-changing-the-world-order/; Andy Greenberg, "How an Entire Nation Became Russia's Test Lab for Cyberwar," Wired, June 20, 2017, https://www.wired.com/story/russian-hackers-attack-ukraine/; Scott Shane and Mark Mazzetti, "The Plot to Subvert an Election: Unraveling the Russia Story So Far," *New York Times*, September 20, 2018, https://www.nytimes.com/interactive/2018/09/20/us/politics/russia-interference-election-trump-clinton.html; and Kim Zetter, "An Unprecedented Look at Stuxnet, the World's First Digital Weapon," Wired, November 3, 2014, https://www.wired.com/2014/11/countdown-to-zero-day-stuxnet/.

[10] United Nations Security Council (UNSC), *Final Report of the Panel of Experts Established Pursuant to Resolution 1874 (2009)* (New York: UNSC, March 5, 2019), https://www.ncnk.org/sites/default/files/UN_POE_March2019_Final_Report.pdf; Council on Foreign Relations (CFR) Cyber Operations Tracker, *Compromise of TV5 Monde*, (Washington, DC: CFR, April 2015), https://www.cfr.org/cyber-operations/compromise-tv5-monde; Russell Brandom, "How a DDoS Campaign Became an Act of Cyberwar," Verge, March 24, 2016, https://www.theverge.com/2016/3/24/11301876/ddos-iran-banks-dam-prosecution-indictment; and Peter Elkind, "Sony Pictures: Inside the Hack of the Century," *Fortune*, June 25, 2015, https://fortune.com/longform/sony-hack-part-1/.

[11] John Costello, "China's Irregular Warfare in the Cyber Domain," Real Clear Defense, June 17, 2015, https://www.realcleardefense.com/articles/2015/06/18/chinas_irregular_warfare_in_the_cyber_domain_108094.html.

[12] Gregory J. Rattray and Jason Healey, "Non-State Actors and Cyber Conflict," in *America's Cyber Future: Security and Prosperity in the Information Age*, vol. 2 (Washington, DC: Center for a New American Security, 2011), 65–86; and Ben Whitham, "Exterminating the Cyber Flea: Irregular Warfare Lessons for Cyber Defence," in *Proceedings of the 13th Australian Information Warfare and Security Conference* (Perth, Western Australia: Security Research Institute, Edith Cowan University, 2012).

[13] Gregory J. Rattray and Jason Healey, "Non-State Actors in Cyber Conflict," in *Addressing Cyber Instability*, ed. James C. Mulvenon and Gregory J. Rattray (Vienna, VA: Cyber Conflict Studies Association [CCSA], 2012).

[14] Frank C. Sanchez, Weilun Lin, and Kent Korunka, "Applying Irregular Warfare Principles to Cyber Warfare," *Joint Force Quarterly* 92 (1st Quarter 2019): 15–22, https://ndupress.ndu.edu/Portals/68/Documents/jfq/jfq-92/jfq-92_15-22_Sanchez-Lin-Korunka.pdf.

from counterterrorism efforts to cyber conflict.[15] David Raymond addresses the paradoxes of counterinsurgency as this article does, but he focuses on tactical and technical aspects, gleaning lessons for offensive and defensive military cyber operators.[16]

That counterinsurgency may hold central lessons to deal with cyber conflict is suggested by a single sentence from John Nagl's forward to the original Army and Marine Corps field manual on counterinsurgency, "while firepower is the determinant of success in conventional warfare, the key to victory in counterinsurgency is intelligence on the location and identity of the insurgent enemy derived from a supportive population."[17] This sentence hits on the three similarities of counterinsurgency strategy to cyber conflict: adversaries are hidden and depend on deception; the conflict is fought in and among the populace (and with a host nation); and the relationship between superior firepower and long-term success is not as straightforward as it is in the modern system of warfare.

Deception and the Role of Intelligence

In both counterinsurgency and cyber conflict, adversaries try to remain hidden and rely extensively on deception for success. Surprise attacks and ambushes are the norm rather than the exception and most cyber capabilities and operations are unthinkable without a healthy dose of deception.[18] When it discusses attacks from adversaries, US military cyber doctrine frets the "design of the Internet lends itself to anonymity and . . . attribution will continue to be a challenge for the foreseeable future."[19] Of course, this difficulty of attribution is beneficial when the United States military is looking for a "low probability of detection" for its own offense and espionage.[20]

In a phrase very similar to those used by cyber commanders, the Army's latest FM 3-24 offers a clear assessment, "Effective counterinsurgency operations are shaped by timely, relevant, tailored, predictive, accurate, and reliable intelligence. . . . Without accurate and predictive intelligence, it is often better to not act rather than to act."[21] A key goal of intelligence is to take away the insurgent's ability to hide,

[15] Michael Senft, "Lessons Not Learned: Why Our Post-9/11 Counterterrorism Experiences Should Inform Our Cybersecurity Strategy," Modern War Institute, February 28, 2019, https://mwi.usma.edu/lessons-not-learned-post-9-11-counterterrorism-experiences-inform-cybersecurity-strategy/.

[16] David Raymond, "Paradoxes of (Cyber) Counterinsurgency," *Cyber Defense Review*, February 9, 2015, https://cyberdefensereview.army.mil/CDR-Content/Articles/Article-View/Article/1136129/paradoxes-of-cyber-counterinsurgency/.

[17] John A. Nagl, "The Evolution and Importance of Army/Marine Corps Field Manual 3-24, Counterinsurgency," in *The U.S. Army/Marine Corps Counterinsurgency Field Manual*, Headquarters, Department of the Army (HQDA) (Chicago: University of Chicago Press, 2007).

[18] Erik Gartzke and Jon R. Lindsay, "Weaving Tangled Webs: Offense, Defense, and Deception in Cyberspace," *Security Studies* 24, no. 2 (2015): 316–48, https://deterrence.ucsd.edu/_files/Weaving%20Tangled%20Webs_%20Offense%20Defense%20and%20Deception%20in%20Cyberspace.pdf.

[19] JCS, *Cyberspace Operations*, Joint Publication 3-12, (Washington, DC: JCS, June 8, 2018), I-12.

[20] JCS, *Cyberspace Operations*, IV-8.

[21] HQDA, *Insurgencies and Countering Insurgencies*, Field Manual (FM) 3-24 (Washington, DC: HQDA, 2014), I-19.

whether in complex terrain or among the population. This has a clear application to cyber conflict in which adversaries develop their attack and command-and-control infrastructure in "gray space" and mix their attacks and exfiltration of stolen data into legitimate traffic flows. Moreover, in both cyber and counterinsurgency there may be very thin lines distinguishing what is an intelligence operation versus a purely military operation.

Host Nation and Populace

"The host nation doing something tolerably is normally better than us doing it well," states the original FM 3-24.[22] The goal is to work by, with, and through partners who are closest to the threat and may have unique capabilities and knowledge of the local culture, geography, and human terrain.

The same holds true for cyber conflict. The only difference is the host nation is the collection of key cybersecurity companies like Symantec, FireEye, and CrowdStrike; network service providers like AT&T, Verizon, and NTT; and major information technology vendors like Microsoft, Intel, and Cisco. The private sector not only owns the vast majority of this critical infrastructure but it is on the front lines of the battle against nation-state attackers and makes the vast majority of critical decisions to thwart them. While uneven, the analogy is still useful. The key counterinsurgency problem is identifying insurgents and separating them from the population. The host nation is often a deeply imperfect partner in this task, lacking capabilities and with differing goals and perspectives than the United States.

By contrast, in cyber the private sector often has *superior* capabilities. Few if any major cybersecurity incidents have been solved by government actions.[23] Rather, the major technology and cybersecurity companies of the private sector—AT&T, Verizon, Symantec, FireEye, and CrowdStrike—have the agility, subject matter expertise, and ability to change cyberspace directly to resolve incidents decisively, usually while the government is still arguing about what should be done and which agency has the right authority. The New York Cyber Task Force found private sector actions like automatic vulnerability updates and patching, end-to-end encryption, and cloud-based security have been the most effective at shaping the terrain of cyberspace in favor of defenders and reducing sanctuaries at scale.[24]

These companies are digital natives—their entire organizations are built around the mission of creating and shaping cyberspace. The cyber offense and intelligence organizations of the US government would face significant organizational, budget, authority, and mindset challenges

[22] HQDA, *Counterinsurgency Field Manual*, FM 3-24 (Washington, DC: HQDA, 2006), I-27–I-28.

[23] Jason Healey, ed., *A Fierce Domain: Conflict in Cyberspace, 1986 to 2012* (Vienna, VA: CCSA, 2013).

[24] New York Cyber Task Force, *Building a Defensible Cyberspace* (New York: Columbia University School of International and Public Affairs, September 2017), https://sipa.columbia.edu/sites/default/files/3668_SIPA%20Defensible%20Cyberspace-WEB.PDF.

replicating such strengths and generally only visit cyber terrain built and maintained by others.

The private sector can of course be an imperfect partner, conflicted by its pursuit of profit. But these flaws are no more severe than the government's own internal and interagency conflicts. Trade and diplomatic priorities have often trumped those of cybersecurity as has pursuing national interests through offensive cyber capabilities for the US Intelligence Community, military, and law enforcement.

Governments have their own unique and very powerful strengths: massive resources of national budgets and workforces, staying power to remain committed for years to resolve seemingly intractable problems, and additional authorities and levers of national power, including intelligence, diplomacy, and the military. Rather than trying to replicate the strengths of the private sector at great financial cost, the US government must hitch its advantages to those of the private sector.

Beyond the partnership with the host nation, successful counterinsurgency also requires a supportive population to recognize the legitimacy of the host nation and US forces. Cyber conflict may be like counterinsurgency in this way: if you lose moral legitimacy, you lose the war. If so, the US government needs to win the hearts and minds of the global population of netizens.

Cyber actors of all kinds—from criminals up to apex predators like the United States, Russia, and China—hide their infrastructure in "gray space," which the military describes as "those portions of cyberspace" which are neither "protected by the US" nor "owned or controlled by an adversary or enemy."[25] The use of this polite euphemism obscures the fact that gray space is mostly private property—devices, computers, and networks purchased and operated by people and companies around the world. Treating this private property merely as gray space reduces it to little more than a square on the chessboard of the never-ending game of constant contact between adversaries.

Especially after the Snowden revelations about the scale and intrusiveness of US espionage, the US legitimacy to play this game in the role of a defender has been challenged.[26] One frequent response, which might be summarized as, "of course US intelligence agencies are going to spy; don't hate the player, hate the game," might be true but misses the point that people have a unique and exquisitely personal relationship with their technology. This is not the Cold War when spy-versus-spy played out in Geneva or Moscow. Gray space holds our deepest secrets and connects us to beloved family members and intimate friends.

It may be true that spies are going to spy, other intelligence agencies operate with fewer restrictions, or Americans reveal far more intimate secrets—with less protection—to tech companies. It also may not

[25] JCS, *Cyberspace Operations*, I-4–I-5.

[26] Lawfare, "Snowden Revelations," Lawfare (blog), n.d., https://www.lawfareblog.com/snowden-revelations.

matter. Retired Air Force General and former director of both the National Security Agency and the Central Intelligence Agency Michael Hayden warned even entirely legal cyber operations conducted with proper oversight can suffer a lack of perceived legitimacy. After the Snowden revelations, many Americans said: "'You know, I'm not so sure that constitutes consent of the governed anymore. That may actually be consent of the governors. You may have told them but you didn't tell me.'"[27] The same dynamics led to citizens of Allied nations pressuring their governments to reduce security cooperation with the United States, which seemed to have no respect for their privacy.[28]

Firepower

Many of the paradoxes of counterinsurgency deal with firepower and the use of force. "Sometimes, the more force is used, the less effective it is. . . . military actions by themselves cannot achieve success. . . . The more successful the counterinsurgency is, the less force can be used and the more risk must be accepted."[29]

Until recently, the United States has been similarly hesitant to use cyber capabilities. Successive administrations have been concerned attacks might cascade or cause unknowable collateral damage, adversaries might concentrate attacks against vulnerable US cyber-connected infrastructure, or attacks would work against the preferred US goals for "an open, interoperable, secure and reliable cyberspace."[30] US cyber forces were only given relatively free rein against the Islamic State, so long as cyber actions did not take place outside "the declared areas of active hostilities" in Iraq, Syria, and Afghanistan.[31]

No longer. In 2018, then National Security Adviser John Bolton boasted the restraints on cyber response had been lifted: "Our hands are not tied as they were in the Obama administration."[32] The new cyber strategy gave US Cyber Command more leeway to "pursue attackers across networks and systems," "continuously engaging and contesting

[27] Michael Hayden, interview by Glenn Thrush, "Politico's Glenn Thrush Interviews Michael Hayden," *Politico*, March 28, 2016, https://www.politico.com/story/2016/03/full-transcript-politicos-glenn-thrush-interviews-michael-hayden-221275.

[28] Natasha Lomas, "Europe's Top Court Strikes Down 'Safe Harbor' Data-Transfer Agreement with U.S.," TechCrunch, October 6, 2015, https://techcrunch.com/2015/10/06/europes-top-court-strikes-down-safe-harbor-data-transfer-agreement-with-u-s/.

[29] HQDA, *Counterinsurgency Field Manual*, I-26–I-28.

[30] Barack Obama, *International Strategy for Cyberspace: Prosperity, Security, and Openness in a Networked World* (Washington, DC: White House, May 2011), 3, https://obamawhitehouse.archives.gov/sites/default/files/rss_viewer/international_strategy_for_cyberspace.pdf.

[31] Dina Temple-Raston, "How the US Hacked ISIS," National Public Radio, September 26, 2019; and *United States Cyber Command: Hearing before the United States Senate Committee on Armed Services*, 115th Cong. (May 9, 2017), https://www.armed-services.senate.gov/hearings/17-05-09-united-states-cyber-command.

[32] John Bolton, "National Security Adviser John Bolton on Cyber Strategy (Audio Only)," September 20, 2018, https://www.c-span.org/video/?451807-1/national-security-adviser-bolton-briefs-cyber-strategy-audio-only.

adversaries" and to "degrade the infrastructure . . . that enable[s] our adversaries to fight in cyberspace."[33]

A direct implied relationship exists between the military's aggressive use of cyber force and defeating—or at least disrupting or dissuading—adversaries.[34] But just because this makes traditional military sense does not mean it will work. As with counterinsurgency, there may be an inverse relationship between firepower and outcomes. Civilians cannot evacuate the front lines of cyberspace; the Internet is an infrastructure built around commercial and cultural needs. The caution displayed by past US administrations in employing offensive cyber operations may not have been intended to create mere bureaucratic hassle but may have been a legitimate procedural step to prevent escalation, miscalculation, and mistakes.

There are at least three clear reasons to keep cyber rules of engagement tight. First, the negative impact on legitimacy resulting from only one or two errant shots in an area crowded with civilians—and fragile critical infrastructure—can outweigh the dozens, hundreds, or thousands that hit true, as the United States learned after accidentally bombing Afghan weddings.[35] Second, US adversaries might benefit from the relative low cost of developing capabilities, easily keeping pace with the United States and leading to escalation. Third, if adversaries in cyberspace believe they are retaliating against a strike initiated by the United States, they are more likely to attack US military operations. And if DoD networks are too well defended, adversaries will simply target the private sector. This is not mere conjecture—after the US-Israeli Stuxnet attack on Iran's uranium enrichment program, the Iranians did not retaliate against the Mossad, the Central Intelligence Agency, or the US military, but instead attacked American banks.[36]

Recommendations

Some risks resulting from a forward defense posture with fewer operational restrictions are worth taking in cyber conflicts in order to achieve gains. Several recommendations follow that will help manage these risks.

First, the US government must treat the "host nation"—the major IT and cybersecurity companies—as the supported command, rather than insisting the military has some unique "secret sauce"—in the

[33] Mark Pomerleau, "New Authorities Mean Lots of New Missions at Cyber Command," Fifth Domain, May 8, 2019, https://www.fifthdomain.com/dod/cybercom/2019/05/08/new-authorities-mean-lots-of-new-missions-at-cyber-command/; USCYBERCOM, *Achieve and Maintain Cyberspace Superiority: Command Vision for US Cyber Command* (Fort Meade, MD: USCYBERCOM, 2018), 6; Jason Healey, "Triggering the New Forever War, in Cyberspace," Cipher Brief, April 1, 2018; and Nakasone, "Cyber Force," 11.

[34] Jason Healey, "The Implications of Persistent (and Permanent) Engagement in Cyberspace," *Journal of Cybersecurity* 5, no. 1 (2019): 5, https://academic.oup.com/cybersecurity/article/5/1/tyz008/5554878.

[35] BBC South Asia, "US 'Killed 47 Afghan Civilians,'" BBC News, July 11, 2008, http://news.bbc.co.uk/2/hi/south_asia/7501538.stm.

[36] Ellen Nakashima, "Iran Blamed for Cyberattacks on U.S. Banks and Companies," *Washington Post*, September 21, 2012.

words of an early commander of US Cyber Command—enabling it to be the center of American cyber defenses.[37] This support must go far beyond bland public-private partnerships—often more subordination than alliance—or defense support to civil authorities. In the defense support to civil authorities model, "the military's cyber capabilities will be available to civilian leaders to help protect the networks that support government operations and critical infrastructure," just as "during a natural disaster, like a hurricane, military troops and helicopters are often used by [the Federal Emergency Management Agency] to help deliver relief."[38]

Responding to major cyber incidents is not akin to delivering relief, it is active contention with an agile adversary working predominantly in private-sector networks. Accordingly it demands a new model. Erik Korn and I recently described one possibility, "defense support to the private sector," through which critical infrastructure sectors on the front lines make direct calls for fire from the private sector, task the Intelligence Community with requirements, coordinate multi-stakeholder defensive actions, and rely on direct support by new military formations tailored to each critical infrastructure sector.[39]

Second, the Department of Defense and Intelligence Community need to focus more on winning the support of domestic and foreign audiences—not just other governments and elites, but netizens as well. It is no longer enough, if it ever was, to defend US operations by saying our adversaries show even less restraint, all is fair in intelligence collection, or the issue is leaks about US operations and not the operations themselves. If the lessons of irregular warfare hold, then the United States must be accepted as a legitimate defender of cyberspace, a task hard to accomplish merely through the more aggressive or sustained use of offensive and intelligence cyber operations.

Third, the Department of Defense needs to be cautious in its enthusiasm regarding the role of firepower in case disrupting adversaries just emboldens enemies and alienates friends. Defending forward must be treated as an operational experiment, not settled wisdom: try something, measure what works, abandon what does not, repeat.

Fourth, the National Security Council should moderate the authorities granted to US Cyber Command with a sunset clause and require specific metrics for success and failure: How long will success

[37] Shane Harris, *@War: The Rise of the Military-Internet Complex* (New York: Houghton Mifflin Harcourt, 2014), 158.

[38] William J. Lynn III, "Remarks on Cyber at the RSA Conference," (speech, RSA Conference, San Francisco, CA, February 15, 2011), https://archive.defense.gov/speeches/speech.aspx?speechid=1535.

[39] Jason Healey and Erik B. Korn, "Defense Support to the Private Sector: New Concepts for the DoD's National Cyber Defense Mission," *Cyber Defense Review*, special edition (2019): 227–42, https://cyberdefensereview.army.mil/CDR-Content/Articles/Article-View/Article/2035015/defense-support-to-the-private-sector-new-concepts-for-the-dods-national-cyber/.

take, and how will we know it when we see it?[40] If these key questions cannot be answered, then authorities which enable defending forward must be scaled back lest the United States create another open-ended forever war, this time in cyberspace and with nuclear-armed adversaries.

It is entirely possible, perhaps even likely, a never-ending string of generals will testify, as they did for Iraq and Afghanistan, that we are "turning the corner" in cyberspace, and just one more military push will lead to success. Before the new strategy becomes too entrenched, these leaders should pause to remember counterinsurgency doctrine that reminds us, "sometimes doing nothing is the best reaction," as it can be easy to overreact.[41] There may simply be no military solution to countering adversary cyberattacks against the United States.

[40] Jason Healey, "Memo to POTUS: Responding to Cyber Attacks and PPD-20," The Cipher Brief, May 24, 2018, https://www.thecipherbrief.com/column_article/memo-potus-responding-cyber-attacks-ppd-20.

[41] HQDA, *Counterinsurgency Field Manual*, I-27.