GAVIN WILDE, NON-RESIDENT FELLOW

Understanding and countering cyber threats

- An updated U.S. cyber strategy should incorporate lessons learned about the nature and limitations of offensive cyber capability—operations which "deceive, degrade, disrupt, deny, destroy, or manipulate" adversary systems—which has proven most effective at espionage and disruption and less as a decisive element of warfare.[1]
- A continued military-centric approach to cyber issues risks underemphasizing the other core competencies of U.S. statecraft—intelligence, diplomacy, law enforcement, and other tools—necessary to address illicit cyber activity like ransomware and state-backed hacking.
- The most persistent and enduring threats from the cyber domain are best addressed through investments in law enforcement, civil infrastructure, public-private resiliency, and international coalitions—less through military superiority.

The federal government's cyber organizational structure

Source: Senate Republican Policy Committee

Created in 2021, the Office of the National Cyber Director is supposed to synchronize and oversee federal cyber policy. However, with few formal powers and an annual budget of only $250,000, it will be difficult for the office to provide meaningful oversight or coordinate federal cyber policy from the White House.

The cyber landscape U.S. strategy currently conceives

- The U.S. faces formidable nation-state adversaries in cyberspace. China, Russia, North Korea, and Iran have all demonstrated capabilities to hold U.S. interests at varying degrees of risk—from intellectual property to democratic institutions to state secrets.
- Non-state and semi-state actors, like hacktivists, ransomware collaboratives, private surveillance companies, and cyber criminals, have also grown in sophistication—disrupting routine economic, governmental, and civic interactions.
- The U.S. strategy currently conceives of cyberspace as a militarized, warfighting domain—evinced by the standup in 2010 of DoD's Cyber Command and its more recent guiding principles: "Defend Forward" and "Persistent Engagement," prioritizing assertiveness in disrupting malicious cyber activity, even below the level of armed conflict.[2]
- This concept fuels debates over "offense vs. defense" in cyberspace, a false binary that distracts from the need to confront cyber issues holistically, using the most appropriate tools and authorities available to the U.S. government for the discrete types of threats they pose. Relative to other departments and agencies, however, the preponderance of resources is dedicated to DoD.[3]

[1] "Cyber Electromagnetic Activities," U.S. Department of the Army, February 12, 2014, https://irp.fas.org/doddir/army/fm3-38.pdf.
[2] "Achieve and Maintain Cyberspace Superiority: Command Vision for US Cyber Command," U.S. Cyber Command, April 2018, https://www.cybercom.mil/Portals/56/Documents/USCYBERCOM%20Vision%20April%202018.pdf; Jason Healey, "The Implications of Persistent (and Permanent) Engagement in Cyberspace," *Journal of Cybersecurity* 5, no. 1 (2019), https://academic.oup.com/cybersecurity/article/5/1/tyz008/5554878.
[3] Jason Healey, "The Cyber Budget Shows What the U.S. Values—And It Isn't Defense," Lawfare, June 1, 2020, https://www.lawfareblog.com/cyber-budget-shows-what-us-values%E2%80%94and-it-isnt-defense.

The limits of offensive cyber

- The relatively muted success of Russian cyber operations in achieving its military and political aims in Ukraine in 2022 call into question notions about cyber as a decisive, coercive element of modern war and suggest a more ancillary role.[4]
- More broadly, in pursuing both battlefield and strategic political objectives, nation-states largely fail to demonstrate in practice the decisive power cyber weapons provide in theory: deterrence, compellence, escalation dominance, or signaling.[5] Kinetic weapons offer more speed, control, and intensity[6] during a conventional armed conflict.
- The primary threat to the U.S. from both nation-state and non-state cyber actors stems from their increasing capacity to conduct more traditional forms of interstate competition: surveillance, espionage, subversion, deception, and disruption, all of which occur below the level—and often in lieu of—conventional armed conflict.
- The most prevalent forms of malicious activity in cyberspace—often incorrectly portrayed as "attacks"—are less measures of war and more of an unending intelligence contest expanding into the digital realm to seek advantage through espionage and subversion.[7] This was the case with the notorious SolarWinds hack in which the Russian foreign intelligence service leveraged a software supply-chain to spy on a broad range of prominent public and private downstream targets.[8]
- Competing and defending in this environment requires partnerships spanning civil society and industry. DHS's Cybersecurity and Infrastructure Security Agency (CISA) is poised to establish such a multi-stakeholder task force to counter ransomware, building on the progress of extant private sector initiatives and leveraging competencies that are often beyond the resources and remit of governments—and outside the scope of warfighting.[9]
- While sophisticated cyber operations targeting U.S. critical infrastructure threaten major disruptions to economic and civil activity, a military-led response may not be best suited such discrete risks—contrary to U.S. Cold War and post-9/11 political reflexes.[10]
- U.S. cyber strategy should thus de-emphasize military- and battlefield-centric notions of offensive superiority and instead center around more effective aims of coalition-building to raise collective cyber-defenses and build operational capacity among stakeholders in critical infrastructure and business. These efforts will both help prevent and speed recovery from cyber incidents.

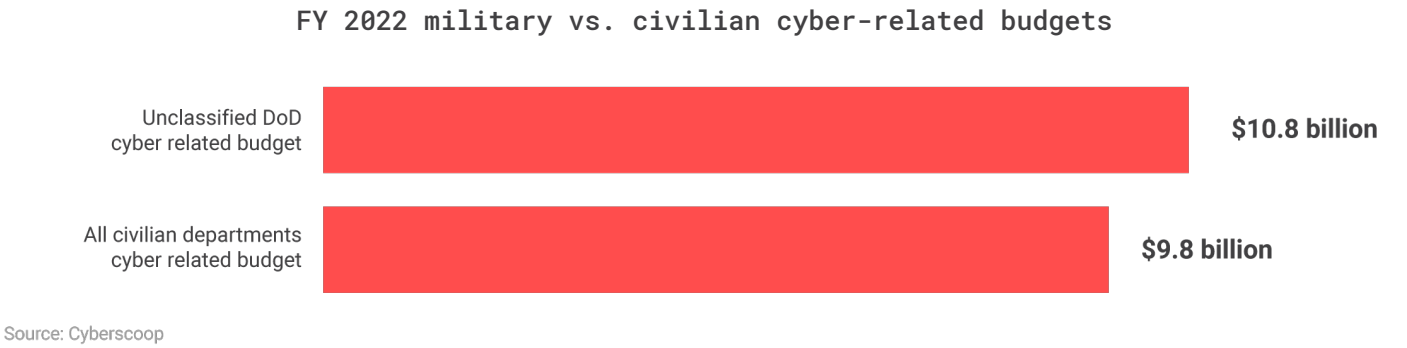
Right-sizing the military role in U.S. cyber statecraft

- Civilian and law enforcement agencies, like CISA, DOJ, FBI, and Department of State made major strides in recent years toward preventing, disrupting, and prosecuting illicit transnational cyber activity.[11]
- Such successes are often forged with interagency, international, and industry partnerships with verifiable results.[12] They demonstrate that addressing issues like ransomware and botnets as national security concerns requires neither militarizing the nature of the threat nor deputizing DoD as a digital police force.[13]

---

[4] "Russia's Failure in Cyberspace," School of Public Diplomacy, March 18, 2022, https://spp.gatech.edu/news/item/656475/russia-failure-cyberspace.
[5] Brad D. Williams, "Nakasone: Cold War-style Deterrence 'Does Not Comport to Cyberspace,'" *Breaking Defense*, November 4, 2021, https://breakingdefense.com/2021/11/nakasone-cold-war-style-deterrence-does-not-comport-to-cyberspace/.
[6] Lennart Maschmeyer, "The Subversive Trilemma: Why Cyber Operations Fall Short of Expectations," *International Security* 46 no. 2 (Fall 2021): 51–90, https://direct.mit.edu/isec/article/46/2/51/107693/The-Subversive-Trilemma-Why-Cyber-Operations-Fall.
[7] Joshua Rovner, "Cyber War is an Intelligence Contest," *War on the Rocks*, September 16, 2019, https://warontherocks.com/2019/09/cyber-war-as-an-intelligence-contest/; Jon R. Lindsay, "Cyber conflict vs. Cyber Command: Hidden Dangers in the American Military Solution to a Large-scale Intelligence Problem," *Intelligence and National Security* 36, no. 3 (October 2020): 1–19, https://www.researchgate.net/publication/346517926_Cyber_conflict_vs_Cyber_Command_hidden_dangers_in_the_American_military_solution_to_a_large-scale_intelligence_problem.
[8] Lily Hay Newman, "A Year After the SolarWinds Hack, Supply Chain Threats Still Loom," *Wired*, December 8, 2021, https://www.wired.com/story/solarwinds-hack-supply-chain-threats-improvements/.
[9] Adam Janofsky, "U.S. Agencies Announce Initiatives to Crack Down on Ransomware," The Record, May 20, 2022, https://therecord.media/joint-ransomware-task-force-doj-cryptocurrency-cyber-initiatives/.
[10] Brandon Valeriano and Benjamin Jensen, "The Myth of the Cyber Offense: The Case for Restraint," Cato Institute no. 862, January 15, 2019, https://www.cato.org/sites/cato.org/files/pubs/pdf/pa862.pdf.
[11] Hollie Hennessy, "CISA Alert on ICS, SCADA Devices Highlights Growing Enterprise IoT Security Risks," Dark Reading, April 15, 2022, https://www.darkreading.com/omdia/cisa-alert-on-ics-scada-devices-highlights-growing-enterprise-iot-security-risks; Joe Warminsky, "U.S. Says It Disrupted Russian Botnet 'Before It Could Be Weaponized,'" Cyber Scoop, April 6, 2022, https://www.cyberscoop.com/russian-botnet-disrupted-garland-doj/; "Russian Hacker Sentenced to Over 7 Years in Prison for Hacking into Three Bay Area Tech Companies," U.S. Department of Justice, September 30, 2020, https://www.justice.gov/usao-ndca/pr/russian-hacker-sentenced-over-7-years-prison-hacking-three-bay-area-tech-companies.
[12] "CISA, FBI, and NSA Release Cybersecurity Advisory on Russian Cyber Threats to U.S. Critical Infrastructure," U.S. Cybersecurity and Infrastructure Security Agency, January 11, 2022, https://www.cisa.gov/uscert/ncas/current-activity/2022/01/11/cisa-fbi-and-nsa-release-cybersecurity-advisory-russian-cyber; "Four Russian Government Employees Charged in Two Historical Hacking Campaigns Targeting Critical Infrastructure Worldwide," U.S. Department of Justice, March 24, 2022, https://www.justice.gov/opa/pr/four-russian-government-employees-charged-two-historical-hacking-campaigns-targeting-critical.
[13] Kristen Eichensehr, "Friction, Framing & U.S. Cybersecurity-Related Actions Against Russia," *Just Security*, April 7, 2022, https://www.justsecurity.org/81027/friction-framing-department-justice-cybersecurity-related-actions-against-russia/; Gavin Wilde, "On Ransomware, Cyber

- These breakthroughs notwithstanding, funding for U.S. military cyber operations dwarfs the combined cybersecurity budgets of all other agencies combined.[14] The NDAA, DoD's annual authorization bill, is also, concerningly, becoming the sole vehicle via which other departments and agencies can overcome congressional gridlock to secure funding for their own cyber initiatives.[15]
- Meanwhile, the authorities under which DoD conducts cyber operations are subject to decreasing civilian oversight, a sharp contrast with those necessary for other military operations.[16] Previously, Cyber Command's offensive cyber operations reportedly required presidential approval and interagency coordination prior to execution.[17]
- A 2018 White House directive—the details of which are classified and were withheld from congressional review by the Trump Administration—reportedly relegated these authorities to DoD.[18] The Biden administration examined further refinements to these authorities that would lend additional weight to the diplomatic ramifications of overseas operations.[19]
- Like concerns over unconstrained drone warfare, it is unclear whether a more aggressive, unilateral military posture in cyberspace is strategically sound policy—it may risk further inflaming the very domain it seeks to pacify.[20] In both cases, technological advances lower the barriers to entry into military conflict without enabling decisive victory within it.
- This mismatch in cyber budget, oversight, and authorities creates competing incentives within a national cyber strategy and risks both distracting and overextending the military from its core warfighting competencies into less existentially vital aspects of global competition.
- Future U.S. strategy should redirect resources toward capacity-building among civilian and law enforcement agencies to enable better prevention, disruption, and resilience. It should likewise reconceptualize DoD's role as an adjunct, not a centerpiece, of U.S. cyber statecraft.



Source: Cyberscoop

DoD's cyber-related budget, even excluding classified expenditures, exceeds the budget for all civilian departments combined. This reflects the over-militarization of U.S. cyber policy.

A new organizing principle for U.S. cyber strategy

- The ambiguity the cyber domain affords makes it highly attractive to nation-states seeking alternatives to conventional war. This is not a failure of a deterrence, but rather a workaround due to deterrence's effectiveness.
- The cyber domain's capacity to land decisive blows amidst conventional conflict has also proven thus far to be a less viable prospect than previously envisioned.[21]

Command Should Take a Backseat," *Just Security*, November 30, 2021, https://www.justsecurity.org/79361/on-ransomware-cyber-command-should-take-a-backseat/.

[14] Jason Healey, "The Cyber Budget Shows What the U.S. Value—And It Isn't Defense," Lawfare, https://www.lawfareblog.com/cyber-budget-shows-what-us-values%E2%80%94and-it-isnt-defense.

[15] Michael Garcia, "The Militarization of Cyberspace? Cyber-Related Provisions in the National Defense Authorization Act," Third Way, April 5, 2021, https://www.thirdway.org/memo/the-militarization-of-cyberspace-cyber-related-provisions-in-the-national-defense-authorization-act.

[16] Suzanne Smalley, "Biden Administration Is Studying Whether to Scale Back Trump-era Cyber Authorities at DoD," Cyber Scoop, March 31, 2022, https://www.cyberscoop.com/biden-trump-nspm-13-presidential-memo-cyber-command-white-house/.

[17] Chris Bing, "Trump Administration May Throw Out the Approval Process for Cyberwarfare," Cyber Scoop, May 2, 2018, https://www.cyberscoop.com/ppd-20-white-house-national-security-council-cyber-warfare-tactics/.

[18] Hon. Paul C. Ney, Jr, "DOD General Counsel Remarks at U.S. Cyber Command Legal Conference," U.S. Department of Defense, March 2, 2020, https://www.defense.gov/News/Speeches/Speech/Article/2099378/dod-general-counsel-remarks-at-us-cyber-command-legal-conference/.

[19] Suzanne Smalley, "State to Gain More Ability to Monitor DoD Cyber Ops under White House Agreement," Cyber Scoop, May 10, 2022, https://www.cyberscoop.com/state-to-gain-authorities-to-monitor-dod-cyber-ops-under-new-white-house-agreement/.

[20] Daniel DePetris, "Reevaluating U.S. Targeted Killing Policy," Defense Priorities, January 27, 2022, https://www.defensepriorities.org/explainers/reevaluating-us-targeted-killing-policy; Myriam Dunn Cavelty, "The Militarisation of Cyberspace: Why Less May Be Better," 2012 4th International Conference on Cyber Conflict (2012): 141–153, https://ccdcoe.org/uploads/2012/01/2_6_Dunn-Cavelty_TheMilitarisationOfCyberspace.pdf.

[21] Ciaran Martin, "Cyber Realism in a Time of War," Lawfare, March 2, 2022, https://www.lawfareblog.com/cyber-realism-time-war.

- Casting warfare as the organizing bureaucratic and conceptual substrate to U.S. cyber power and strategy risks underservicing the other elements of national power, including legal, economic, intelligence, and diplomatic efforts that have proven effective to securing and advancing U.S. interests in cyberspace.
- A more durable framework would place robust cyber defense, multi-stakeholder resiliency, and coalition-based statecraft of our own at its core.