Jacquelyn G Schneider, PhD

Hoover Fellow, Hoover Institution, Stanford University

U.S. MILITARY STRATEGY AND DOMESTIC POLICY COORDINATION

Testimony before the U.S.-China Economic and Security Review Commission

Hearing on China's Cyber Capabilities: Warfare, Espionage, and Implications for the United States

February 17, 2022

Distinguished members of the Commission, thank you for the opportunity to speak with you today. I have been asked to talk about U.S. military cyber strategy and capabilities and to give my assessment about our force posture to combat the Chinese cyber threat. I want to make it clear that I am here in my civilian capacity as a Hoover Fellow at the Hoover Institution and do not speak on behalf of the U.S. government or the Department of Defense. Additionally, all my assessments come from public and unclassified documents and therefore I want to caveat that there may be U.S. military capabilities and operations that are not open source and therefore are not within the realm of my analysis.

Today I am going to give an overview of the evolution of the Department of Defense cyber strategy leading up to the 2018 concepts of "persistent engagement"[1] and "defend forward."[2] I will outline continuities and changes in assumptions within these strategies and assess their success. I will then detail more concretely how the U.S. military has built and organized its cyber capabilities and whether these capabilities and organizations are optimized to combat the Chinese cyber threat. Finally, I will conclude with policy recommendations for the U.S. military as it continues to deal with a growing Chinese cyber threat.

Department of Defense Cyber Strategy Overview

We can trace the Department of Defense's first real cyber strategy to July 2011, almost a full year after the creation of U.S. Cyber Command—what was then a sub-unified command under Strategic Command.[3] This 2011 strategy represented the DoD's first nascent attempt at organizing and prioritizing what was an extremely profound and uncertain "new" cyber domain. As such, the strategy is a starting point for how the U.S. military should think about cyber—more of a declaration that cyber mattered than an articulation of priorities, threats, or lines of effort. Unlike later versions of the DoD's cyber strategies, no adversaries are named explicitly and the document is as much concerned with non-state and insider threats as any one particular nation-state. It is also quite vague about how the U.S. military will combat the threat. This

[1] https://www.cybercom.mil/Portals/56/Documents/USCYBERCOM%20Vision%20April%202018.pdf?ver=2018-06-14-152556-010
[2] https://media.defense.gov/2018/Sep/18/2002041658/-1/-1/1/CYBER_STRATEGY_SUMMARY_FINAL.PDF
[3] https://csrc.nist.gov/CSRC/media/Projects/ISPAB/documents/DOD-Strategy-for-Operating-in-Cyberspace.pdf

vagueness is likely a representation of the larger uncertainty that existed a decade ago about the role that the U.S. military would play in cyberspace as well as the Department of Defense's relationships with other federal agencies in combating cyber threats. Nevertheless, the document foreshadows a continuity across U.S. cyber strategies over the next decade, including a clear prioritization of "protecting and respecting the principles of privacy and civil liberties, free expression, and innovation" while mitigating the vulnerabilities of the department's reliance on digital technologies.

The 2011 DoD cyber strategy came on the heels of the Obama Administration's International Cyberspace Strategy which articulated a largely optimistic view of cyberspace as an environment with a clear collective good for humanity—a perspective informed by the Arab Spring. Accordingly, the strategy sought to uphold the universal good of an open and interoperable, secure and reliable cyberspace primarily through norms, diplomacy, active law enforcement, as well as dissuasion and deterrence. The document called for little from the Defense Department, asking the military simply to "recognize and adapt to the military's increasing need for reliable and secure networks, build and enhance existing military alliances, and to expand cyberspace cooperation." Even the document's understanding of deterrence was predicated largely on resilience and proportional threats of punishment, promising to "reserve the right to use all necessary means—diplomatic, military, and economic—as appropriate and consistent with applicable international law ... we will exhaust all options before military force whenever we can; we will carefully weigh the costs and risks of action and of inaction; and will act in a way that reflects our values and strengthens our legitimacy and international support whenever possible."[4]

The four years after both of these 2011 strategies saw an exponential increase in the scope, severity and diversity of cyber hacks and attacks. It also saw four years of learning and building, in which the U.S. government focused on creating a unified federal approach to cyberspace (the infamous bubble chart which laid out the primary roles and responsibilities for DOD, DHS, Department of State, and the FBI/DOJ).[5] The Obama administration developed and articulated normative principles about appropriate behaviors in cyberspace (such as a norm against attacks on critical infrastructure), and focused on propagating these norms within the United Nations and relationships with allies.[6]

This rise in cyber threats as well as the evolution of U.S. government roles and responsibilities led to a significantly more mature 2015 Defense Department Cyber Strategy.[7] This is the first defense strategy to identify priority adversaries (namely Russia, China, Iran, North Korea, and non-state actors), to articulate the Department of Defense's responsibilities within the federal government, and to lay out defense cyber lines of effort. There are similarities across the 2011 and 2015 strategies. Most notably for the DoD, the 2015 strategy still focused mostly on norms and deterrence to combat cyber threats. The document called for the Defense Department to "be prepared to" defend the U.S. homeland and to "build and maintain viable

---

[4] https://obamawhitehouse.archives.gov/sites/default/files/rss_viewer/international_strategy_for_cyberspace.pdf
[5] "Cyber Strategy and Policy," *Committee on Armed Services, United States Senate, One Hundred Fifteenth Congress, First Session,* March 2, 2017.
[6] https://2009-2017.state.gov/secretary/remarks/2015/05/242553.htm
[7] ttps://media.defense.gov/2018/Sep/18/2002041658/-1/-1/1/CYBER_STRATEGY_SUMMARY_FINAL.PDF

cyber operations" in order to "control escalation." This strategy focused on responding to and preparing for cyber incidents and leaned heavily on deterrence—by denial and vague threats of punishment—as the primary line of effort for ensuring the open and secure use of cyberspace.

Government responses to cyber incidents from 2011 to 2015 centered mostly on economic, diplomatic and legal activities, and the Department of Defense was largely postured to support[8] other agencies rather than acting on its own. As former Secretary of Defense Chuck Hagel asserted in 2014, the Pentagon "will maintain an approach of restraint to any cyber operations outside the U.S. Government networks. We are urging other nations to do the same."[9] The Defense Department's 2015 cyber strategy may have primarily placed DoD cyber capabilities in a reserve and deter posture, however, they were experiencing exponential growth: 133 new cyber mission teams were developed, and four service cyber commands began to equip, train and operate cyber forces to support operations on the air, land and sea.[10]

I want to highlight that this first period was a period of relative restraint in U.S. military responses to cyber threats, and, coming into the Trump administration in 2018, state sponsored cyber activity was in no way slowing down. The Obama Administration was very concerned about the risks of escalation from U.S. military cyber operations including cyber network exploitation and therefore offensive cyber operations played a very limited role in the overarching cyber strategy. Leading into the Trump Administration and after the Russian hack-and-release and disinformation campaigns of the 2018 election,[11] there was a push from within both the private sector and the Department of Defense for a more active and forward leaning strategy.[12] In response, in 2018 the U.S. rewrote all of its cyber strategies and moved from a diplomacy deterrence-first, "be prepared" stance under the Obama Administration to a forward-leaning, risk acceptant, and active strategy under the new administration. In particular, the 2018 summary of the Department of Defense's Cyber Strategy introduced the concept of "defend forward," confronting adversaries before cyber-attacks even occur "to disrupt or halt malicious. cyber activity at its source, including activity that falls below the level of armed conflict."[13] In general, the Trump Administration's approach was highly decentralized, giving much more autonomy and responsibilities to the Department of Defense and Cyber Command (which was now elevated to a unified command).[14]

There were a few core assumptions that changed from 2015 and 2018. The first was an assumption about cyber risk. Whereas the Obama Administration had assumed that cyber operations were inherently escalatory, the Trump Administration believed the risk from adversary cyber attacks outweighed the potential risks of escalation. This led the administration to delegate more authorities down to the military. Secondly, whereas the previous. strategies had

---

[8] http://nationalsecurity.gmu.edu/wp-content/uploads/2018/05/Alexander-Testimony-A-Borderless-Battle.pdf
[9] https://archive.defense.gov/Speeches/Speech.aspx?SpeechID=1837
[10] https://www.defense.gov/News/News-Stories/Article/Article/1524747/cyber-mission-force-achieves-full-operational-capability/
[11] https://www.washingtonpost.com/technology/2018/12/16/new-report-russian-disinformation-prepared-senate-shows-operations-scale-sweep/
[12] https://www.academia.edu/34619726/Navy_Private_Sector_Critical_Infrastructure_War_Game_Report
[13] https://warontherocks.com/2018/09/defending-forward-the-2018-cyber-strategy-is-here/
[14] https://www.defense.gov/News/News-Stories/Article/Article/1966758/esper-describes-dods-increased-cyber-offensive-strategy/

focused on deterring and responding to cyber events, the new DoD cyber strategy and Cyber Command vision (colloquially nicknamed persistent engagement) presented cyber as a more or less constant competition below a threshold of armed conflict. This was a key assumption for the DoD as it framed cyber operations (both offensive and defensive) as pre-conflict, non-geographic problems. This is important because it carves out an operational space for the new Cyber National Mission Forces to plan and execute cyber campaigns outside of the joint planning or combatant command process. Finally, whereas the Obama Administration outlined five priority actors in its 2015 defense cyber strategy, the 2018 focuses more narrowly on China and Russia as the primary competitors and therefore the focus of cyber efforts.

This newfound defense cyber autonomy, combined with very operationally focused leaders like new commander, General Nakasone, led to large scale experimentation in Department of Defense cyber operations. Meanwhile, the Department of Homeland Security leaned forward under new leadership in its Cyber and Infrastructure Security Agency, ushering in a much more publicly responsive face to cybersecurity and new partnerships with both the private sector and the Department of Defense. Cyber Command and the Cyber and Infrastructure Security Agency began to release information about malware and threats broadly and created new operational structures centered around issue-specific task forces (for instance election security) that appeared to be relatively successful. Meanwhile, Cyber Command used its new authorities to develop new missions like "hunt forward,"[15] which sent U.S. cyber troops into allied and partner networks to search for adversary activity and to grow the new Cyber Mission Force (in both mandate and personnel).

Despite the maturation of U.S. cyber strategy over the last decade, there are still elements that are inconsistent or underdeveloped. The first issue is clarity. Unclear language (in particular the concepts of defend forward and persistent engagement) within Department of Defense strategies and Cyber Command Vision led onlookers to question what military cyber was really doing. While public statements[16] and DOD-sponsored articles[17] painted a picture of defend forward that included cyber defense teams in allied states or intelligence sharing with private sector, unofficial reports by the New York Times[18] suggested U.S. was placing malware exploits in Russian critical infrastructure. This led onlookers to question how far forward exactly the U.S. was defending. Faced with this ambiguity, some critics worried the U.S.' new strategic concept could inadvertently lead to retaliation, potentially violent.

At its core the ambiguity in language represented a two-threshold logical inconsistency within U.S. strategy. The U.S. wanted to deter adversaries from taking cyber attacks against the U.S., going so far in the 2018 Nuclear Posture Review[19] as to imply that cyber attacks *could* be responded to with nuclear retaliation. However, it didn't hold its own actions to the same threshold. In fact, in its own strategy, the U.S. asserted that most cyber attacks were below a "threshold of armed conflict" and therefore that the U.S. intended to conduct undefined cyber

---

[15] https://www.cybercom.mil/Media/News/Article/2433245/hunt-forward-estonia-estonia-us-strengthen-partnership-in-cyber-domain-with-joi/
[16] https://www.fifthdomain.com/smr/cybercon/2019/11/12/heres-how-cyber-command-is-using-defend-forward/
[17] https://ndupress.ndu.edu/Portals/68/Documents/jfq/jfq-92/jfq-92.pdf
[18] https://www.nytimes.com/2019/06/15/us/politics/trump-cyber-russia-grid.html
[19] https://media.defense.gov/2018/Feb/02/2001872886/-1/-1/1/2018-NUCLEAR-POSTURE-REVIEW-FINAL-REPORT.PDF

actions prior to conflict without anticipating retaliation. The ambiguity in language made it hard to differentiate between what cyber attacks were appropriate and which were inappropriate, suggesting the U.S. might have different interpretations about what it believed it could do in cyberspace versus what its adversaries could do.[20] This analytical slippage had secondary effects on deterrence credibility as it called into question whether the U.S. was really willing to punish (up to nuclear weapons) for cyber attacks.

Beyond the logical inconsistencies, even those who supported defend forward voiced concern that these operations could become never ending task forces, expensive to sustain, and difficult to tell whether they were more or less effective.[21] This leads to the second real problem with U.S. cyber strategies across time. None of these cyber strategies outlined how to assess whether the strategy or its implementation was more or less effective. Even the 2018 Joint Publication 3-12 on cyberspace operations (the Department of Defense's more or less guidebook on how it organizes and U.S.es cyber capabilities) punts on measures of performance in cyberspace, declaring that "development of operational-level MOPs/MOEs (measures of performance/measures of effectiveness) for CO (cyber operations) is still an emerging aspect of operational art."[22] Additionally, all of the strategies struggled to articulate time horizons, a problem when assessing their effectiveness. Cyber Command's vision of persistent engagement intentionally downplays the role of events or time-bounded crises in cyber strategy, but also fails to delineate any differentiation between short term and long term effectiveness for the vision For example, Obama Administration efforts at the end of their term to clamp down on Chinese IP theft in cyberspace were initially successful; however, five years later Chinese IP theft is on the rise at potentially greater levels than seen before 2015.[23] Does that mean that defend forward wasn't a successful strategy?

Finally, while all of the DoD cyber strategies so far have prioritized the need for an open, free, and secure internet; they stop short at identifying the DoD's role in safeguarding valid information. What role, if any, should the DoD play in combatting campaigns of disinformation or the manipulation of data to degrade trust in economic or governance systems? The DoD has devoted cyber capabilities to foreign disinformation campaigns against COVID[24] as well as foreign campaigns of electoral disinformation. However, disinformation scholars find it difficult to disaggregate many foreign disinformation campaigns from domestic. This complex relationship between foreign and domestic actors in disinformation complicates the scope of DoD authorities when it comes to combatting disinformation. Future strategies will have to assess what the appropriate role for the DoD should be in these information campaigns.

Department of Defense Cyber Capabilities and Posture

---

[20] Schneider, Jacquelyn. "A strategic cyber no-first-use policy? Addressing the U.S. cyber strategy problem." *The Washington Quarterly* 43, no. 2 (2020): 159-175.

[21] https://cisac.fsi.stanford.edu/news/herb-lin-and-max-smeets-what-absent-us-cyber-command-vision; https://www.lawfareblog.com/persistent-engagement-foundation-evolution-and-evaluation-strategy

[22] JP 3-12, July 2018, pg. IV-22.

[23] https://www.wsj.com/articles/china-violated-obama-era-cybertheft-pact-u-s-official-says-1541716952

[24] https://www.defense.gov/News/News-Stories/Article/Article/2147566/DoD-works-to-eliminate-foreign-coronavirU.S.-disinformation/

The last ten years of DoD cyber strategy shaped U.S. cyber capabilities—both defensive and offensive. So how is the U.S. military's cyber force organized and how do we understand what U.S. military cyber capabilities are? There are many layers of cyber forces within the DoD. At the highest level are the joint organizations—Cyber Command and the Defense Information Systems Agency. Cyber Command is a 4-star level functional command whose commander, Gen Nakasone, also leads the National Security Agency. Cyber Command, like any functional command, is in charge of the larger joint bureaucratics of cyber operations: planning, joint cyber intelligence, coordinating operations, equipping and generating the force. It also, unique to a functional command, is in charge of its own Cyber National Mission Force (CNMF), which includes teams who "defend the nation by seeing adversary activity, blocking attacks, and maneuvering in cyberspace to defeat them."[25] This force, which includes National Mission Teams, National Support Teams, and National-level Cyber Protection Teams is in charge of "protection of non-DODIN blue cyberspace."[26] In other words, CNMF is in charge of DoD operations to defend and protect non-military cyber targets within the United States. They are, therefore, the primary lead on defend forward operations designed to protect U.S. critical infrastructure. It is a bit unclear what this means in practice, but could include counter-cyber attacks against nation states and foreign non-state actors that might target the United States.

Cyber Command is in charge of coordinating all DoD cyber activities. This coordination extends to defense: for example, in generating cyber protection teams and creating defensive strategies. It also includes coordinating with the Defense Information Systems Agency and the Joint Force Headquarters-Department of Defense Information Network. DISA is run by a three star, currently Air Force General Lt Skinner, who is also in charge of Joint Forces Headquarters—Department of Defense Information Network (JFHQ-DODIN). DISA can be thought of as the DoD's joint enterprise level manager of information systems. They are in charge of enterprise level network architecture and information technology management as well as "defensive cyber operations—internal defensive measures"[27] which include vulnerability assessments and incident response analysis.

[25] https://sgp.fas.org/crs/natsec/IF10537.pdf
[26] JP 3-12, July 2018, pg. I-9.
[27] DISA Fiscal years 2019-2022 Strategic Plan Version 2, pg. 14: https://disa.mil/-/media/Files/DISA/About/Strategic-Plan.ashx.

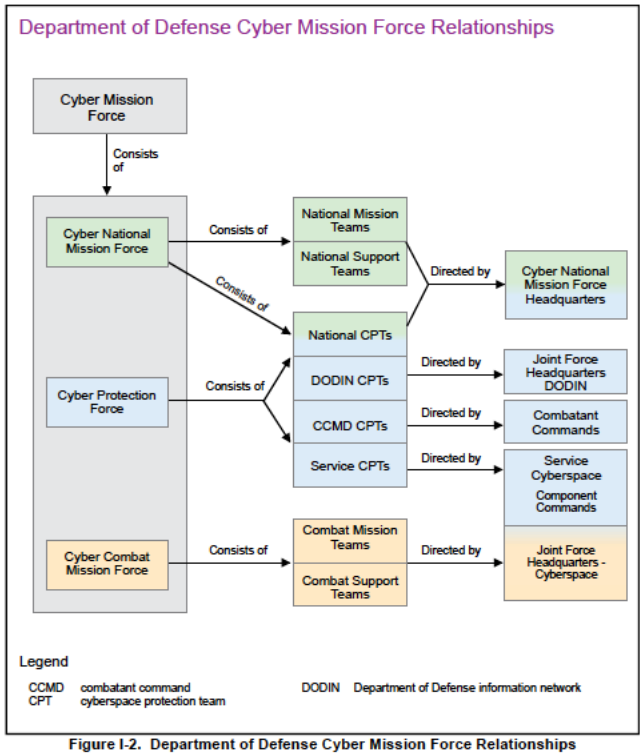

Figure I-2. Department of Defense Cyber Mission Force Relationships

[28]

In addition to DISA, the Department of Defense also has a Chief Information Office which includes the Deputy Chief Information Officer for Cybersecurity who is in charge of "the integration of Defense-wide programs to protect the Department's critical infrastructure against advanced persistent threats, and assures coordination of cybersecurity standards, policies, and procedures with other federal agencies, coalition partners, and industry. The DCIO CS organizes and implements DoD efforts to transform the cyberspace workforce in support of U.S. national security priorities."[29]

[28] JP 3-12, July 2018, pg. I-10.
[29] https://DoDcio.defense.gov/about-DoD-cio/organization/dcio-cs/

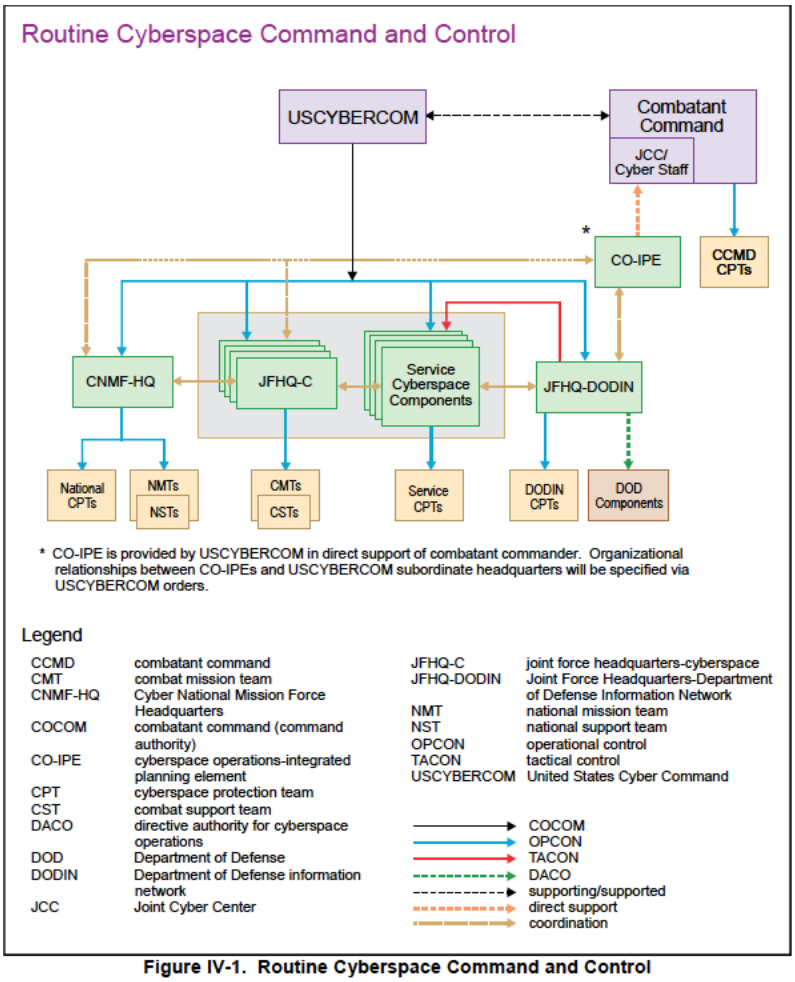

Figure IV-1. Routine Cyberspace Command and Control

These organizations are all joint. However, most of the DoD's cyber funding and manpower actually resides in each of the respective armed services cyber components. Cyber Command is lead for the Cyber Mission Force; Army Cyber,[30] 10th Fleet,[31] the 16th Air Force,[32] and MARFOR Cyber[33] are the service leads. Each of the services has its own cyber mission teams which are dedicated to service-specific missions, whether those are in defense (cyber protection teams) or offense (cyber mission teams). Service cyber teams often focus on domain-specific targets: for instance, the 16th Air Force may specialize in cyber operations that support air campaigns by taking down radars or integrated air defense systems. In contrast, the 10th Fleet, may be concerned with cyber support to the aircraft carrier or anti-submarine warfare. Resources to develop offensive capabilities usually reside at the service cyber level (minus those resources allocated specifically to the Cyber National Mission Force). The armed services also own their own networks and data so each service has its own version of a CIO office as well as units devoted to cybersecurity on their service networks.[34] This means that there is large variation in both cyber offense and defense within each of the armed services.

[30] https://www.arcyber.army.mil/
[31] https://www.fcc.navy.mil/
[32] https://www.16af.af.mil/About-U.S./Fact-Sheets/Display/Article/1957318/sixteenth-air-force-air-forces-cyber/
[33] https://www.marforcyber.marines.mil/
[34] https://warontherocks.com/2021/12/the-air-force-isnt-doing-it-right/

The armed services own most of the personnel, resources, and infrastructure that man and equip DoD cyber. However, the geographic component commands use some of these service cyber resources in support of combatant plans and operations. Like in the other domains, there is an inherent tension between the manning and resources allocated at the functional level (Cyber Command) and within the armed services and what the combatant commanders have available to execute their combatant operations.

What does this all mean for U.S. military cyber capabilities? Measuring cyber capabilities is extremely difficult. Whereas in other domains capability is measured by orders of battle, performance in exercises, physical defense measures, or even the kinetic effects of different weapon systems—cyber capabilities are virtual, rarely static, difficult to predict their effect, and quite often classified. We therefore turn to proxies like number of personnel, maturity of organizations or doctrine, resident expertise, or past examples as a crude way to estimate capabilities. Using these proxies to evaluate US military cyber capabilities reveals some clear strengths and weaknesses.

First and foremost, the U.S. has perhaps the most mature cyber doctrine of any other country in the world. Additionally, U.S. Cyber Command and the service cyber elements have become the exemplar for military cyber institutional growth. Despite the institutional growth of U.S. military cyber, the U.S. is by no means the largest cyber force by number of personnel. Although it is difficult to estimate the entire DoD cybersecurity workforce, the military arm of the Cyber Mission Force includes 133 teams of approximately 6,000 personnel.[35] This is a far smaller number than estimates of the PLA's cyber workforce which can be as large as 50,000-60,000.[36] Additionally, the U.S. has struggled to attract and retain cyber talent in the military,[37] a challenge which all of the previous DoD cyber strategies discuss in depth. Finally, we know based on open source reporting that the U.S. has sophisticated cyber accesses and exploits.[38] It is unclear, however, the extent of these capabilities, partly because there are very few historical examples of known U.S. cyber exploits (especially ones that have significantly changed the course of a crisis or conventional military campaign). Similarly, defensive capabilities are difficult to assess. Government accountability office reports have critiqued the Defense Department for cyber vulnerabilities in weapons systems[39] and there are public reports of successful hacks against the Department of Defense—most notably the Russian led Solarwinds hack[40] and Chinese backed Microsoft exchange hack.[41] Perhaps critically, an arcane and difficult acquisitions process has made it difficult for the DoD to keep up with cutting edge commercial cybersecurity technology[42] while the byzantine bureaucratic administration of DoD networks has made it difficult to implement enterprise-wide cybersecurity solutions.[43]

---

[35] https://www.c4isrnet.com/cyber/2021/05/14/will-the-cyber-mission-force-soon-receive-more-personnel/
[36] https://www.nationaldefensemagazine.org/articles/2021/3/3/mumbai-incident-spotlights-chinas-cyber-capabilities
[37] https://digital-commons.U.S.nwc.edu/cgi/viewcontent.cgi?article=1044&context=U.S.nwc-newport-papers
[38] https://www.iiss.org/blogs/research-paper/2021/06/cyber-capabilities-national-power
[39] https://www.gao.gov/products/gao-19-128
[40] https://www.nytimes.com/2020/12/14/U.S./politics/rU.S.sia-hack-nsa-homeland-security-pentagon.html
[41] https://apnews.com/article/microsoft-exchange-hack-biden-china-d533f5361cbc3374fdea58d3fb059f35
[42] https://fcw.com/acquisition/2021/11/why-dod-is-so-bad-at-buying-software/259180/
[43] https://taskandpurpose.com/news/air-force-cybersecurity-nicolas-chaillan/

China: Cyber Competition and Conflict

What does all of this mean for U.S. and China, especially through the lens of competition or conflict? First, China is an able cyber adversary that harnesses a large workforce, extensive research in data and information networks, and who has shown a willingness to use cyber operations to steal intellectual property and exploit sensitive information. In a crisis or violent conflict, China would likely use these cyber capabilities to attack American command, control, and communications as well as vulnerable digitally enabled weapons systems. While Chinese doctrine a decade ago suggested the PLA might conduct cyber attacks against American critical infrastructure early in a crisis, more recent discourse suggests that China is concerned about its own critical infrastructure as well as escalation risks of targeting American civilians. These factors may induce restraint and limit Chinese cyber attacks on American critical infrastructure.

There is an inherent tension between developing U.S. military cyber forces to combat Chinese status quo cyber operations and preparing cyber capabilities for a U.S.-China crisis or conflict. On the one hand, countering Chinese intellectual property theft and network exploitation focuses on public-private partnerships, cyber defense, and broad national resiliency—potentially with the addition of counter cyber operations that target PLA cyber units or government sponsored hackers. These types of responsibilities would mostly reside with the Cyber National Mission Forces. In contrast, focus. on cyber capabilities for a conflict with China means devoting resources to cyber accesses and exploits within China's conventional military forces, command and control, and potentially that dual-use infrastructure that China might rely on to move and supply troops and weapons. These types of cyber missions would primarily be conducted by service cyber elements in conjunction with the combatant commands. Optimizing military cyber for status quo competition with China suggests prioritizing the Cyber National Mission Forces and Cyber Command over the geographic commands while focusing on cyberspace resources for military conflict with China prioritizes geographic commands. None of the cyber strategies so far have delineated priorities amongst these missions but manpower and resource limitations suggest that it will be hard the U.S. to devote adequate resources to both of these missions (as well as emerging challenges with disinformation campaigns, ransomware, and ongoing attacks from Russia, North Korea, and Iran).

Absent an ability to prioritize between a force postured for cyber competition with China versus a force focused on building targets and capabilities to use in a conflict, the U.S. military should invest in cyber capabilities that extend across competition and conflict: cyber defense, information and network resilience, and counter-cyber capabilities. None of these lines of effort are new to U.S. cyber strategy; the 2018 strategy introduced the concept of defend forward as a way to counter China in competition and conflict and talked explicitly about investments in defense and resiliency. However, it's unclear whether the U.S. has implemented or prioritized these lines of effort in its cyber posture against China. There is no open source reporting to suggest the U.S. has exercised defend forward by conducting offensive cyber operations to degrade PLA cyber capabilities. While the Cyberspace Solarium Commission recommended greater partnerships between the DoD and the defense industrial base, to include a threat hunting initiative, there is no evidence that either DoD or defense industrial base networks are less vulnerable than they were four years ago. Chinese intellectual property theft and network exploitation has

increased since the last cyber strategy, suggesting that either the strategy or the implementation is not working against the status quo China cyber threat.

Policy Recommendations

What should the U.S. military do in order to better prepare its cyber force for both status quo competition and conflict with China?

The solution starts with resilience, or as Dr. Erica Borghard explains, "the ability to anticipate and withstand a disruptive event, and to rapidly restore core functions and services in its wake, whether it be a pandemic, financial crisis, terrorist attack, or large-scale cyber incident."[44] Resilience requires not only investing in networks and technologies that are more technically resilient, but also in building data users that are more resilient. For the Department of Defense, this involves building networks that gracefully degrade and campaigns that can be executed with limited access to data. At the core for any data user, whether it is a military officer, a federal civilian, or an American citizen is building human resilience—educating data users to question their data's biases, to look at data sources, and to have a back-up plan in place when they don't have access to digital resources.

Tied intimately to resilience are three activities: defense, intelligence, and information sharing. All three of these activities benefit from investments in commercial technology, as well as federal investment in research and development in cybersecurity. The DoD's struggle to modernize software procurement, development, and sustainment has an outsized negative effect on cybersecurity. Further, the Biden administration should continue to build out the interagency and public-private information sharing that matured over the Trump Administration. There continue to be difficulties sharing information between the public sector and defense; continued investments in clearinghouses and procedures to automate this information sharing will lead to better cyber defense for both the DoD and U.S. industry writ large.

The DoD should also use a new cyber strategy as an opportunity to resolve some of the ambiguity and logical inconsistencies of the 2018 strategy. Here the Biden Administration has a real opportunity with China—not only to ensure the success of its own strategy, but also to build norms of appropriate behavior in cyberspace. To do this a new strategy first needs to announce to adversaries and allies what is off limits, and subsequently deter these strategic cyber-attacks by threatening credible retaliation options. We've come close to this before. The Obama Administration crafted an Executive Order on sanctions[45] in response to cyber-attacks on critical infrastructure and Trump's State Department has called out cyber-attacks on health infrastructure as inappropriate behavior in cyberspace. However, the U.S. has always stopped short of binding its own hands or credibly threatening anything beyond sanctions or tit for tat cyber punishment for these cyber-attacks.

This is partially because the U.S. has been too expansive in what it has deemed as "off limit" cyber targets for adversaries. The Obama Administration's definition of critical infrastructure spanned 14-16 sectors and both Administrations have struggled to define what

[44] https://warontherocks.com/2021/01/a-grand-strategy-based-on-resilience/
[45] https://home.treasury.gov/policy-issues/financial-sanctions/sanctions-programs-and-country-information

kinds of cyber operations against these infrastructures they seek to deter. If everything is important, then nothing is important. Absent an understanding of what the U.S. cares about in cyberspace, ambiguous cyber deterrence by punishment policies have been unable to stem the increasingly prolific and sophisticated wave of cyber operations against U.S. civilian enterprises.

The first step, therefore, in solving the U.S. cyber strategy problem is to decrease strategic ambiguity about what cyber-attacks are serious enough to warrant a violent response from the U.S. To date, the U.S. has not resorted to violence in response to cyber-attacks, even though the U.S. has threatened up to nuclear response to cyber-attacks. Instead of these ambiguous threats, the U.S. needs to focus strategic deterrence on the cyber-attacks which are the most likely to have credible deterrence options. This is a high bar. Most cyber-attacks will not be able to be credibly deterred, but the U.S. may be able to credibly threaten cross-domain punishment for truly strategic cyber-attacks: those that create violent effects against civilian populations or threaten a state's nuclear control. At this high strategic level, which is only reserved for the most dangerous cyber operations, the U.S. can credibly threaten its vast and lethal military force and therefore shore up deterrence.

But defining and deterring what the U.S. cares about at the strategic level is only the first necessary step to solving the U.S. cyber strategy problem. The U.S. must not just assert these targets off limits for U.S. adversaries, but also declare them off limits for the U.S. The adoption of a no-first-use cyber strategic attack policy, especially one buttressed by credible threats of retaliation across military options, can help signal credible U.S. restraint and scope appropriate "status. quo" cyber activity, thus shoring up both a strategic threshold of restraint and a lower threshold of status quo cyber activity that occurs without violent retaliation. Both of these thresholds are essential for the current U.S. cyber strategy to succeed. And while a no first use policy was never adopted in the nuclear world, there are important differences in cyberspace that make no first use more credible and more advantageous. than in the nuclear domain.

While the adoption of a no first use strategic cyber-attack policy will help shore up strategic restraint, the U.S. will have to go beyond no first use in order to ensure strategic success. It must also pair strategic no first use policy with clearer statements about what types of activities fall under defend forward—thus making both ends of the cyber spectrum less ambiguous and more defined. Ideally, defend forward is a concept scoped to include only counter-cyber operations against cyber adversaries and not to target adversary civilian infrastructure. While defend forward may include up to offensive cyber activity, a clearer articulation of the focus of defend forward activities should help assure adversaries (and allies) that the U.S. will restrain these attacks and not target civilian infrastructure preemptively. This may help to solve the U.S. strategy's hypocrisy problem and correct the logical inconsistencies of an otherwise ambiguous defend forward. All of these actions support norms that the strategy should propagate about what are responsible actions in cyberspace—what is off limits (for U.S. and our adversaries) and where we need to invest in resiliency, defense, and punishment to make cyber exploits less likely to succeed.

Finally, the DoD will have to carve out of an already tight budget investments in crisis response, cyber support to conventional campaigns, and law enforcement. All of these lines of effort require more cybersecurity talent as well as federal funding for technology and

coordination between local governments and federal agencies. The DoD should not be afraid of creative approaches to talent in the federal workforce, including a better use of the military reserves, the development of a civilian reserve corps, and more government fellowships for both academic and industry leaders to contribute to the federal workforce, even for a short time.

These efforts also require a closer look at whether our current planning and organizational structures are optimized for the threat. For example, the development of task forces within Cyber Command was an important innovation that replaced a rigid military campaign planning structure that never worked for cyber. But how do we organize task forces for non-time-delineated tasks like dealing with China? Further, these never-ending task forces are expensive and manpower intensive. How do we know how these task forces should be manned and what is working (or not working)?

The Department of Defense has made significant strides over the last decade to organize, prepare, and combat cyber threats. But China has only become more assertive and willing to use its cyber capabilities to compete with the U.S. economically and militarily. The Department of Defense will have to make difficult decisions to prioritize Chinese cyber threats and to allocate resources to combat status quo cyber operations while also building the reserve cyber capability necessary to combat China in a violent conflict. In the end, what will make the biggest difference will be investments in resiliency, defense, and countering PLA cyber capabilities.