Offensive Cyber Capabilities at the Operational Level

The Way Ahead

PROJECT DIRECTORS
James A. Lewis
J.D. McCreary

AUTHOR
Maren Leed

September 2013

CSIS | CENTER FOR STRATEGIC & INTERNATIONAL STUDIES

Georgia Tech Research Institute

Offensive Cyber Capabilities at the Operational Level

The Way Ahead

Project Directors
James A. Lewis
J.D. McCreary

Author
Maren Leed

September 2013

CSIS | CENTER FOR STRATEGIC & INTERNATIONAL STUDIES

Georgia Tech Research Institute

About CSIS—50th Anniversary Year

For 50 years, the Center for Strategic and International Studies (CSIS) has developed solutions to the world's greatest policy challenges. As we celebrate this milestone, CSIS scholars are developing strategic insights and bipartisan policy solutions to help decisionmakers chart a course toward a better world.

CSIS is a nonprofit organization headquartered in Washington, D.C. The Center's 220 full-time staff and large network of affiliated scholars conduct research and analysis and develop policy initiatives that look into the future and anticipate change.

Founded at the height of the Cold War by David M. Abshire and Admiral Arleigh Burke, CSIS was dedicated to finding ways to sustain American prominence and prosperity as a force for good in the world. Since 1962, CSIS has become one of the world's preeminent international institutions focused on defense and security; regional stability; and transnational challenges ranging from energy and climate to global health and economic integration.

Former U.S. senator Sam Nunn has chaired the CSIS Board of Trustees since 1999. Former deputy secretary of defense John J. Hamre became the Center's president and chief executive officer in April 2000.

CSIS does not take specific policy positions; accordingly, all views expressed herein should be understood to be solely those of the author(s).

About GTRI

For almost 80 years, the Georgia Tech Research Institute (GTRI) has built a reputation as one of the world's premier applied research and development organizations. Each day, GTRI's science and engineering expertise is used to solve some of the toughest problems facing government and industry across the nation and around the globe.

A nonprofit research institute, GTRI teams with its customers to attack their problems with passion and objectivity. In FY 2011, GTRI conducted more than $220 million in sponsored research for government and industry. Our nearly 1,600 expert scientists, engineers, and support staff turn ideas into workable solutions and then put those solutions into action.

GTRI's core research areas are Systems Engineering, Information and Communications Technologies, Sensors and Test & Evaluation. GTRI also has a long history of solving complex problems in the areas of Electronic Warfare, Modeling & Simulation, Materials, Radar, Sensors, Optics, Digital Media, Robotics & Unmanned Systems, Cybersecurity and Aerospace Technologies. Major customers for GTRI research include U.S. Department of Defense agencies, the state of Georgia, nondefense federal agencies, and private industry.

Center for Strategic & International Studies
1800 K Street, NW, Washington, DC 20006
202-887-0200 | www.csis.org

Contents

Acknowledgments

This paper benefitted from the involvement of many experts from across the national security community. The project team is particularly grateful to representatives from each of the military services' cyber, space, electronic warfare and intelligence organizations, U.S. Cyber Command senior staff, representatives of the Office of the Secretary of Defense (both Policy and Intelligence), and legal experts who have served at senior levels in both the intelligence community and senior Defense Department commands. The study team also appreciates the insights from experts at the British Embassy, Australian Ministry of Defense, and various other U.S. government agencies. General James "Hoss" Cartwright (USMC, Ret.) provided a particularly thoughtful review. Any remaining errors are the responsibility of the author alone.

The author and project directors welcome comments and may be contacted as follows:

- Maren Leed, Senior Adviser, Harold Brown Chair in Defense Policy Studies, CSIS, mleed@csis.org;
- James A. Lewis, Director, Technology and Public Policy Program, CSIS, jlewis@csis.org;
- J.D. McCreary, Chief, Strategic Technology Program Office, Sensors and Electromagnetic Applications Lab, Georgia Tech Research Institute, jd.mccreary@gtri.gatech.edu.

Executive Summary

At present, the defense policy landscape is replete with arguments, many of which are ultimately based in the lack of a common vision among both elites and within the broader population about the role of the U.S. military in the future. Cyber operations are one element of these debates, though much of the discussion has centered around how best to defend against a growing cyber threat, the role of the Defense Department in that defense, and tensions between civil liberties and security interests. Occasionally, greater attention is paid to questions about the U.S. use of cyber offensively, which brings with it questions of precedent, deterrence, international norms, and a host of other challenges. But it is also apparent that U.S. leaders have already approved the use of offensive cyber capabilities, though under tight restrictions. While not ignoring this larger context, the specific question this project sought to examine in greater depth is whether the Defense Department should make a more deliberate effort to explore the potential of offensive cyber tools[1] at levels below that of a combatant command.

As we discovered over the course of this effort, perspectives on this question vary widely. Some view lower-echelon offensive interests as a lesser included case of the broader national whole, while others see distinct concerns for division commanders or ship captains, for example, that differ substantially from those that might ever rise to the level of interest of a Combatant Command (COCOM). Such varying views contribute to the reality recently acknowledged by Chairman of the Joint Chiefs of Staff General Martin Dempsey that the roles of the Army, Navy, Air Force, and Marine Corps in cyber warfare remain unresolved.[2]

This project plumbed those varying views and represents an attempt to characterize where the Department of Defense (DoD) stands today and how it might move forward in this area. It starts from the premise that cyber tools offer the potential for operational and tactical commanders to create effects at lower echelons, in support of a broader strategy, that complement existing capabilities. Conceptually, offensive cyber operations offer a source of "fires" whose degree of lethality can be tailored to the situation at hand, be (at least in some instances) reversible, and may prove less costly than alternative methods of pursuing similar effects. The degree to which cyber capabilities can deliver on this promise is debated, but their potential to meet the substantial security challenges that lie ahead is sufficiently promising, especially in comparison to the available alternatives, that the possibility deserves, if not demands, further attention.

This is not to suggest that there are not significant issues associated with the potential use of offensive cyber weapons in general, to include at levels lower than the strategic one that dominates the current debate. This paper seeks to characterize the main arguments both for and against the use of offensive cyber tools at lower echelons. Significant differences of opinion exist on both normative questions but also on issues of fact. With respect to the latter, concerns about offensive cyber in general and tactical cyber in particular have inhibited, to varying degrees, the advancement of capabilities that could better inform their validity. As a result, proponents of exploring the operational and tactical potential of offensive cyber often find themselves trapped by circular logic: the capabilities are not developed, so those who take a more cautious approach argue that considering potential uses is pointless, which perpetuates the lack of clarity about the kinds of conditions under which their use might be considered, so requirements are not clear, so tools are not developed, and so on.

---

[1] For the purposes of this paper, offensive cyber operations are defined as actions that provide instructions not intended by the operator to a processor.

[2] Sydney Freedberg, "Military Debates Who Should Pull The Trigger for A Cyber Attack," BreakingDefense.com, May 22, 2012, http://breakingdefense.com/2012/05/22/military-debates-who-should-pull-the-trigger-for-a-cyber-attack/.

This paper recommends steps to break this cycle by establishing a more explicit plan for robust experimentation. Given where things stand today, it does not recommend that commanders below the level of the commander, U.S. Cyber Command (CYBERCOM), be further empowered to conduct offensive cyber attacks (though they may be in the future). It does, however, describe a general consensus among legal and policy experts that such expansion is theoretically possible, consistent with other military capabilities. It then describes multiple areas that policymakers should and would consider beyond that initial constraint, and the arguments of those who both support and caution against further devolution of offensive cyber authorities. It concludes by acknowledging that the lack of consensus in areas such as technical feasibility, intelligence equities, and capacity and resource requirements suggest that additional experimentation and application is needed, in controlled settings, to enable an informed decision on greater decentralization of attack authorities.

To advance the state of knowledge on technical and other considerations, a necessary prerequisite to any future decisions about greater decentralization of control over the use of offensive cyber tools, the study makes two recommendations: first, that the Office of the Secretary of Defense (OSD) clarify that pursuing offensive cyber capabilities in support of operational and tactical commanders is in fact consistent with current law and policy; and second, that OSD develop an integrated, Department of Defense–wide plan to experiment and exercise with offensive cyber capabilities to support operational and tactical commanders. Implementing such a plan is the only way to better understand the potential benefits, determine the degree to which practical and policy concerns are warranted, and therefore more thoughtfully determine the best way ahead in this poorly understood but possibly revolutionary area.

Introduction

> *Rather than trying to argue over the shape of the table before you know whether the table is valuable, we need to get out there and experiment.*[1]—General James E. Cartwright, 2008

While the future defense budget remains highly uncertain, there is a broad consensus that defense resources will continue to be under pressure. At the same time, defense challenges remain complex, geographically dispersed, and can unfold at unprecedented speed. Against this backdrop, defense policymakers face a range of challenges. First, there is a continuing need to prepare U.S. military forces to operate at scale. Even if a single, large military engagement may seem unlikely (perhaps a North Korean implosion is the most plausible short-term scenario in this regard), the potential for multiple, geographically disparate operations (to include deterrence activities aimed at precluding conflict) calls for capacity across numerous military capabilities. Second, there is a need for strategic depth, or the ability to respond to challenges that could arise almost anywhere on the globe, potentially at speeds unable to be met by traditional military platforms if they are not already in the vicinity. Third, there is the need for a broader range of tools across the diplomatic and military space to respond to challenges arising from weakening state authority, the dispersion of political power, and the diffusion of lethality across a wide range of actors.

The implications of these challenges are significant. Absent sufficient numbers, traditional military systems will have difficulty meeting both the scale and depth requirements of the future. Compressed timelines are leading to the development of highly specialized, and very expensive, niche platforms or military systems. And approaches to address the gap between national and popular interests remain traditional and limited: special operations forces or intelligence capabilities that cannot be easily scaled.

Cyber tools can have numerous attributes that are well aligned to this environment. From a life cycle cost perspective, they can compare very favorably to other weapons systems. All have research and development costs; space programs and traditional platforms also have large production and deployment costs, whereas for cyber weapons these are minimal. Cyber and space weapons have very low operations and maintenance costs, while these can be substantial for traditional weapons systems. In sum, the cost curve for all weapons is initially steep, but it likely falls off quickly for cyber weapons, then space, then traditional platforms.

At least some cyber weapons also have the potential to scale dramatically; a single algorithm could disable a whole class of adversary systems, for example. They can operate at the speed of light, providing a timeliness that is increasingly necessary but difficult to achieve with shrinking inventories of far-flung traditional platforms. Perhaps even more importantly, cyber weapons can have unparalleled versatility. They can operate across the full range of military operations, from engagement to high-end warfare. Because their effects can be reversible, they are well suited to all phases of operation, from shaping the environment through intense warfare through reconstruction. When employed against a specific weapon system, they can counter it at multiple points in time, from early in development (e.g., causing reliability problems) to decisions about employment (disabling even one weapon can introduce doubt about the entire class of weapons in a way that kinetic strikes cannot), up to post-launch or firing. This versatility offers at least one set of capabilities that can operate in the transition space between diplomacy and military action, as well as more squarely in the military domain.

[1] Chuck Paone, "Cartwright at Cyber Symposium: Break Service Barriers," Hanscom Air Force Base 66th Air Wing Public Affairs, June 23, 2008, http://www.hanscom.af.mil/news/story.asp?id=123103885.

The significant asymmetric promise of cyber weapons has been the primary driver behind the U.S. pursuit of offensive capabilities. This has occurred against a backdrop of a larger public discussion about cyber operations that has principally focused on national (and international) cyber policies and, to a lesser extent, the Department of Defense's (DoD's) role in cyber defense. For a variety of reasons, many prefer to focus on the defensive element of the military's role in cyber operations, while discussions of potential offensive use tend to be more circumspect. Despite that reluctance, within the national security community, DoD has recently arrived at high-level rules of engagement for offensive cyber operations. Each of the military Services is an active participant in supporting these strategic cyber activities and is developing forces to support the combatant commands' (COCOMs') cyber priorities. As policies and authorities at the strategic level have been developed and clarified, the services are now turning to a more deliberate consideration of how cyber capabilities might be integrated into future military operations at lower echelons (e.g., Joint Task Force [JTF] and below). Though cyber operations continue to enjoy relative priority as defense resources shrink, one area of relative ambiguity is the degree to which the military services can or should invest in developing cyber capabilities to support military operations below the COCOM level.

This project examined this area in greater detail, seeking to develop a better sense of the potential for operational and tactical cyber operations, as well as to identify the main policy challenges that might influence how fully that potential can or should be realized. It was intended to help advance the policy discussion in this area and to offer insights for consideration in the upcoming Quadrennial Defense Review.

The approach was straightforward. To better understand how lower-level commanders might more fully utilize cyber tools in an operational context, the study teamed convened a classified workshop in June 2013 with representatives from all of the military services, other government agencies, and other technical experts, with expertise inclusive of cyber, electronic warfare, intelligence, surveillance, and reconnaissance (ISR), and kinetic operations across all domains (air, maritime, land, space, and cyber). This workshop resulted in a few key unclassified takeaways. First, the types of cyber effects lower-echelon commanders might wish to create were more expansive and varied than most cyber policy discussions assume. Second, military service representatives all noted some level of institutional resistance to fully exploring the potential for offensive cyber operations at lower levels, though the sources and justifications for that resistance varied.

In July 2013, the study team convened a second, unclassified workshop with policy and legal experts focused on determining what constraints, if any, exist for operational-level offensive cyber use. Though individual perspectives on the wisdom of such employment varied, there was a broad consensus that offensive cyber tools are not subject to constraints beyond those of other types of offensive military capabilities. The discussion below expands upon the issues raised in the two workshops in greater detail and concludes with two recommendations aimed at continuing to move this discussion forward.

Background and Context

Throughout this study, questions were raised about whether there is a meaningful distinction to be made among strategic, operational, and tactical cyber attacks.[2] Some argue, for example, that the nature of cyber suggests that all attacks are potentially strategic in nature, that the fundamental interconnectedness of networks means effects cannot be meaningfully limited,

[2] There is further confusion about whether "tactical operations" means tactical execution in support of a strategically planned operation (i.e., local commanders "triggering" cyber tools implanted previously or forward-deployed forces conducting an attack that can only be accessed through close proximity) or tactical commanders planning and executing cyber operations in support of their own missions in support of higher levels' plans. This paper uses the term in the latter sense.

controlled, or known, and therefore that any given cyber attack, no matter how discretely intentioned, could have massive unintended consequences and poses unknown but potentially significant political risk.

That premise is contested by others who claim that contained operations are in fact possible even within broadly connected systems. They also believe that concerns about the ability to limit effects pertains most directly to wired networks, especially those that are tied to the Internet, and is less directly relevant to closed (which some military systems are) or more localized wireless networks.

This distinction also helps to further illuminate another element of the differences between strategic and operational/tactical cyber targets. Most "strategic" targets (i.e., those that could be expected to have major effects on adversary thinking such that they might prove decisive in the course of conflict) are likely to be "wired and connected." These include target sets like major national command and control networks and their supporting infrastructure, etc. Such targets are also likely to be relatively fixed and presumably well defended in both the physical and cyber domains. But lower-echelon commanders who might wish to use cyber capabilities in a more limited sense (e.g., to deny local communications for a limited period of time, disrupt a maneuver lane by shutting down traffic signals in a portion of a city, or suppress a tactical weapons targeting system) may be more likely to seek to affect wireless networks or targets that rely on local or more circumscribed, closed networks.[3]

From the limited perspective of the nature of any specific "node" that might be the object of a particular cyber attack, any potential target could theoretically be strategic, operational, or tactical, depending on the purpose for which it is used and by whom. Because a "level of war" attribute is not inherent to any given target, it is thus also important to examine the types of effects that various echelons of command might want to create, as well as the conditions under which they might seek to engage with cyber tools.

At all levels, cyber attacks aim to deny, disrupt, or degrade enemy capabilities, either directly or indirectly (e.g., through deception). At the strategic level, commanders are more likely to be interested in large nodes or those with outsized "leverage" in the minds of potential adversaries. Temporary disruption or deception may be sufficient to shape adversary action, but destruction could also be a goal. Almost by definition, these targets are identified in advance, sometimes with years of preparatory work. Tactical commanders, on the other hand, are more likely to wish to employ cyber attacks as part of shaping activities in support of local scheme of maneuver or fires and to be confronted with fleeting or "pop-up" targets that are difficult to anticipate in advance.

Strategic commanders may place a high priority on secrecy and deception as they seek to conduct attacks. The premium for avoiding discovery may be very high, either politically or because of the lost opportunity that would presumably result from any attack being detected "in train." Tactical commanders, on the other hand, may have less need for deception and in at least some instances would place a higher premium on the ability to conduct an attack quickly than on the need to do so without detection.

Therefore, it appears that at a minimum there are a range of targets that vary in their physical nature. Further, our discussions indicate the priorities likely vary across levels of command for the types of desired effects against those targets, as well as the operational conditions that would dictate their utility. By implication, the types of cyber tools that might satisfy the full range of targets, effects, and conditions are widely varied as well.

[3] In practice, no network is truly "closed," because all can be accessed in ways that would enable information transfers through human action. That said, the degree of vulnerability of wired versus "air gapped" networks varies substantially, and the probability that air gaps could be overcome must therefore be part of any determination of the likelihood of spillover effects from any attack.

There is broad agreement that, to date, U.S. Cyber Command (CYBERCOM) and the services' actions in support of the CYBERCOM mission have largely focused on addressing a subset of these targets, those that reflect the priorities of national leaders and, more recently, those of the COCOM commanders. There is further agreement that this focus has been wholly appropriate. But it is also incomplete. The types of targets, effects, and conditions that are reflected in priorities set by COCOM commanders, as is the case with every other kind of type of military capability from intelligence to logistics, will be different from those at lower levels. In the same way that a counter-drug operation might involve the Drug Enforcement Agency concentrating on large-scale, international facilitators, financiers, and distributors, state police focusing on state-wide figures, and a town police department on local dealers in a particular neighborhood, so too do military commanders conduct operations in a nested fashion in support of a broad overall strategic objective.

Practically, the focus on strategic targets suggests a priority on the development of tools that can covertly map, identify vulnerabilities in, and penetrate primarily high-risk, high-payoff targets that likely require long lead intelligence that may result in highly specialized (and therefore very sensitive and fragile) cyber weapons, employed in a scheduled manner. Less attention, however, has been devoted to addressing tactical targets that might be fleeting or opportunistic, less secure, potentially less "connected," and for which there might be a lower premium on covertness or weapon reuse. As one senior officer put it, the former focus necessitates greater attention to "the science of warfighting," while the latter, because it is explicitly designed to react and respond in the midst of ongoing engagements with adversaries, reflects more of its art.

Not surprisingly given the focus to date, the way ahead for addressing the cyber challenges that strategic-level targets present is more clear than is the path to deal with those that represent the target type, effects, and conditions relevant to lower-level commanders. But there are additional issues that currently constrain, or are perceived to constrain, a more comprehensive pursuit of offensive cyber capabilities.

Policy Considerations

Authorities

One of the frequent concerns voiced, to varying degrees, by elements within the all of the military services with whom the study team interacted was that there is insufficient legal or policy authority to permit the use of offensive cyber capabilities at the tactical level. As one recent paper noted, "U.S. policy, authorities, and doctrine for military operations in the cyber domain are not mature."[4] Media accounts indicate that authority for offensive actions is highly centralized within the U.S. government and that decisions involve the president himself.[5] The consensus among the group of legal and policy experts consulted during this study, however, was that while current practice may be to hold approval authorities at very high levels, the potential for commanders at any level to utilize offensive cyber tools during approved military operations is not in fact constrained by either policy or law, as long as existing processes are adhered to.

In the second workshop, experts acknowledged that to date, instances of approval for offensive cyber attacks have been relatively infrequent, and the scope of approval has been narrowly constructed (i.e., against very specific targets, under limited conditions, and with a great deal of scrutiny, and frequently by specialized forces). Again, though, they noted that nothing precludes

[4] Rosemary M. Carter, Brent Feick, and Roy C. Undersander, "Offensive Cyber for the Joint Force Commander: It's Not That Different," *Joint Force Quarterly* 66 (July 2012): 23, http://www.ndu.edu/press/lib/pdf/jfq-66/JFQ-66_22-27_Carter-Feick-Undersander.pdf.
[5] See, for example, David E. Sanger, "Obama Order Sped Up Wave of Cyber Attacks Against Iran," *New York Times*, June 1, 2012, http://www.nytimes.com/2012/06/01/world/middleeast/obama-ordered-wave-of-cyberattacks-against-iran.html?pagewanted=1&_r=0.

that process from being used to consider approvals that are broader in nature. As an example, assuming other constraints were satisfied, if a JTF or subordinate commander wished to employ offensive cyber capabilities as part of an ongoing or future campaign, he or she could request the authority to do so against classes of targets with certain characteristics. That request would be reflected in operational or contingency plans and ultimately in an "Execute Order" (EXORD), all of which would be staffed across the executive branch and ultimately approved by the president or secretary of defense and issued by the chairman of the Joint Chiefs of Staff. (EXORDs routinely include similar types of guidance that apply to other aspects of military action, to include targets that require approvals at higher levels, considerations of collateral damage, etc.) It is this same process that could also be used for a more expansive or more decentralized set of cyber attack authorities if desired.

Though the *process* for broader authority may be sufficient, there are multiple areas of substantive disagreement that affect decisions about whether and how DoD should proceed in this area. They include disparate views on technical feasibility, questions about how to best address intelligence-related impacts of potential offensive cyber actions, and capacity and control issues. Each is briefly addressed below.

Technical Feasibility

Considering the wisdom of decentralized offensive cyber actions is predicated on the assumption that such attacks, like all fires, could actually be executed in ways that are, at a minimum: (1) discrete, that is, tailored to a scale that, through pre-coordination, has been deemed acceptable (e.g., limited to an individual target or class of targets); (2) timely, or that targets are able to be identified, penetrated, and attacked in timelines that are relevant for operational commanders; and (3) sufficiently protective of intelligence equities. Experts disagree on the technical feasibility of at least the first two conditions (the third is addressed more completely below).

As with all weapons, testing is necessary to develop robust understandings of expected effects. For many, whether this is feasible in the cyber realm remains an open question. The basic concern is amplified due to the fact that, unlike many other types of targets, most networks (or portions of networks) are dynamic and constantly changing. These concerns affect the use of cyber weapons at all echelons, and may be one of the main reasons that cyber tools have not been used more broadly to date.

There is disagreement between experts about the feasibility of designing cyber tools that can be reliably employed with confidence about their collateral effects. To some extent this divergence may reflect differences within the broader target environment described earlier. That is, the challenge of limiting or containing effects to the intended target set within a highly networked, potentially globally interconnected system, which may describe many "strategic" targets, is seen as more difficult than doing so against closed systems, that may be only locally accessed, with limited numbers of nodes and/or connectivity that may be more relevant to tactical and operational commanders. Again, this is an empirical proposition that can be tested as a broader tool set is developed and subjected to experimentation. To some extent, these activities are already underway. One of the five technical areas of the Defense Advanced Research Projects Agency (DARPA) "Plan X" program,[6] for example, is explicitly aimed at developing new capabilities in "cyber battlespace analytics," to include measuring and modeling battle damage assessments, in a way that takes the uncertainties inherent in a given network's dynamic aspects into consideration.

Ultimately, the goal would be to develop sets of weapons for preplanned types of operations, much the same as we currently understand and use kinetic weapons and Joint Munitions

[6] An overview of the program's objectives can be found at http://www.darpa.mil/Our_Work/I2O/Programs/Plan_X.aspx.

Effectiveness Manuals (JMEMs) to derive effects-oriented weapons-target pairings, collateral damage analysis, delivery options, and risk analysis.

Timeliness is another major concern. Many argue that, even if effects could be reliably limited, the amount of time it would take to identify, evaluate, and penetrate a given target, particularly if networks or software are frequently changing, would exceed any reasonably expected timeline under which an operational or tactical commander would be operating. Others counter that this is again target dependent, and probably most true for the kinds of targets that are highly protected and interconnected, and for which maintaining secrecy would be of great importance. For lower-level commanders, they may face targets that are less fortified or specialized and that could in theory be actioned much more quickly. Again, Plan X is funding the development of platforms that enable the military to understand, plan, and manage cyber warfare in real-time, dynamic environments, and insights into how well such programs are bearing out will begin to become available in 2014.

In sum, while views differ on whether it is possible to build tools that could be both discrete and timely, there is general agreement that this area, particularly as it relates to lower-priority targets most relevant in a tactical or operational context, remains under-explored. At this stage, it is clear that these capabilities are not robust, but whether they could prove out is just beginning to be more thoroughly examined.

Intelligence Concerns

From an intelligence perspective, tactical use of offensive cyber tools poses at least two major challenges. The first relates to devaluation of the overall cyber toolset. Since using a cyber tool may allow an opponent to develop countermeasures, use in a particular operation may not be the best employment of the tool. Many argue that the potential for significant devaluation of the cyber portfolio as a whole is a decision that only combatant commanders or national authorities are competent to make. Others counter that such cautions are appropriate for highly specialized tools against key strategic targets, but for less strategically valuable targets (e.g., a specific type of adversary vehicle or a local traffic control system), they are less necessary.

The second intelligence concern is that a cyber target may also be an intelligence source that has “customers” up and down the chain of command. If lower-echelon commanders attack certain targets, it could prove very difficult to establish processes that can effectively adjudicate intelligence gain/loss decisions across the multitude of potential stakeholders.

With respect to both challenges, proponents of decentralization argue that the military has developed a well-established targeting cycle that includes legal review, intelligence gain/loss assessment, and other criteria commonly used to evaluate special technical operations that could in theory be adapted to cyber uses as well. In all instances there is a need to decide when the benefits of use outweigh the potential effect on other activities, and therefore a requirement exists to establish the specific forms the decision processes would take to address the interests of all potential stakeholders in a cyber context.

Organization

The final major area of concern with respect to operational and tactical cyber use relates to a basic question of whether the potential benefits outweigh the costs, to include the opportunity costs of resources that could be utilized for other missions. Advocates of continuing along our current path of relatively limited and to some degree ad-hoc development of these capabilities argue that, at present, only the intelligence community and CYBERCOM have the necessary capabilities and resources. If they were to be tasked with expanding their role in this area, it would require either providing additional resources at a time when cuts are the order of the day or diverting attention from current priorities to elevate this area. Nor should any other

organization be tasked with accelerating the development of tactical offensive cyber capabilities, opponents argue, as this would involve building duplicate or redundant capabilities that are unnecessary and unwise in this fiscal environment.

Proponents for the military services taking more deliberate action in the tactical offensive cyber area acknowledge that the National Security Agency (NSA) and CYBERCOM have relevant, and in many cases unique, expertise. However, they believe this expertise is strongest in the areas that relate to strategic-level cyber targets. At least to some degree, therefore, addressing characteristics relevant to targets that are of tactical and operational interest is "uncharted territory," although many of these characteristics align, at least in part, with traditional service competencies in areas that include intelligence, electronic warfare, and space as closely as they do with national intelligence missions, especially the most relevant ones performed by NSA. Thus, proponents claim, new capacity is needed somewhere, and NSA need not be the only source.

The difference of views in this area is related to differing perspectives on "culture." Because of their sensitivity and where competencies currently lie, existing offensive cyber capabilities have been developed almost exclusively in highly classified programs. Some argue that if the United States takes the decision to try to leverage offensive cyber capabilities more fully at lower echelons, this cannot be effectively done while maintaining the current level of classification. That is, if the knowledge of the capabilities of cyber tools is restricted to degrees beyond what typical commanders are authorized to know, those commanders will never fully consider their use in their operational planning.

Further, some argue that the fact that many tools are overseen by intelligence specialists, who may calculate operational value and intelligence loss trade-offs differently than would commanders, which means those decisions are naturally skewed toward preserving intelligence equities. Others counter that the nature of cyber weapons, both as offensive tools and, if reverse engineered, as major vulnerabilities, dictate high levels of classification that cannot be modified without significant and unacceptable levels of risk. They reject the notion that intelligence experts do not fairly represent the trade-offs between immediate operational and both short- and longer-term intelligence value. This tension between "military" and intelligence cultures is not unique to cyber, and it persists not only in debates about the appropriate alignment and relationships between CYBERCOM and NSA, but at lower echelons as well.

Irrespective of future organizational decisions, one area that requires further development is how to manage a cyber "joint operational area," or JOA. JOAs are established to help deconflict fires within a given area and are particularly challenging for cyber because traditional geographic boundaries are much less applicable. There are multiple potential models for how JOAs could be set and managed; this is one of the key areas where experimentation can shed greater light on their relative merits.

Affordability

Irrespective of whether any additional capacity is pursued by CYBERCOM or the military services, all are sensitive to associated resource challenges. As is always the case, the ultimate "cost" to build out these capabilities is highly dependent on how it is done. If operational support is provided in a manner that parallels the current plan for strategic support to the COCOMs, with highly trained and specialized teams, envisioning an affordable way to scale this model is a significant challenge. On the other hand, some foresee, particularly for less challenging targets, a model in which units are able to employ the appropriate cyber tools in a manner more akin to other types of weapons, where the planner understands the capabilities of a given weapon but not necessarily all of the technical and engineering data that underpin that capability. The Navy, for example, has developed a three-tiered system of varying levels of expertise in cyber, with different responsibilities, missions, and training requirements. The feasibility of such an

approach is not yet proven, may need to be adjusted over time, and will likely differ among the services, but refining such an approach could change resource requirements significantly.

More importantly, at this point the discussion about resources is largely premature. In the absence of greater understanding of how capabilities would actually be used, whether they are technically feasible, and how they could be best provided, estimates about eventual resource needs are highly speculative. Advancing the state of knowledge about these questions, however, could (and should) be done iteratively, and this is best pursued through ways that are relatively inexpensive (e.g., through increasing modeling and simulations and dedicating a small numbers of personnel and funding to more deliberate plans of experimentation).

Finally, as noted in the introduction, proponents argue that at the macro level developing this capability could significantly *reduce* costs going forward. As one example, the Navy recently announced plans to deploy a directed energy weapon on one of its amphibious ships.[7] While the laser itself costs in the hundreds of millions, the cost per shot is estimated at less than one dollar, with significant range and other operational advantages. Cost curves for cyber capabilities would likely be similar: costs are concentrated in the development of the tool, with very little expense after that. Actual curves will likely vary, perhaps by target type or effect or condition; collecting data to better understand cost drivers would be a key objective included in experimentation.

Similarly, if a cyber weapon could be used instead of a kinetic weapon to cause a temporary and reversible effect as opposed to a permanent one (e.g., raise a bridge instead of blow it up, or temporarily turn off the lights in a local area instead of destroying a local grid), the United States could theoretically avoid the costs of rebuilding or repairing infrastructure. Whether offensive cyber tools truly offer this type of potential remains uncertain, but if technical and other policy considerations can be resolved going forward, similar types of calculations should be made when assessing cost effectiveness.

Conclusion

With respect to operational and tactical cyber use, the U.S. military finds itself at a logical but difficult decision point. As is historically the case with new technologies, from gunpowder to airpower to space, there is a natural evolution as the capability is introduced, begins to be used, becomes more integrated, and sparks creative thought about further applications. Cyber, and offensive cyber in particular, is moving along this path, which (as has been the case for other technology areas) is fraught with domestic and international legal and policy concerns. The DoD enterprise has rightly focused its attention on addressing these issues at the level where the capabilities can have the most profound effects—the strategic level. But as progress is being made there, the military services are giving more serious consideration to the role that offensive cyber could play in also supporting the priorities of tactical and operational commanders.

To date, the services' efforts have progressed at different rates of speed, due in part to differing service cultures and to the priority placed on the development of these tools by senior leaders within each service. The question for the broader policy community at this point, and for the Office of the Secretary of Defense (OSD) in particular, is whether current efforts are sufficient, or whether a more systematic approach to exploring the potential is warranted. A broader consensus on the wisdom of delegating the authority to use offensive cyber tools may be far in the future, and resolving the many practical concerns explored here is both critical and nontrivial. At present, neither the procedures nor the tools are sufficiently robust to merit a delegation of offensive cyber authorities beyond the very limited ways in which they have been utilized thus far. But a reasonable determination of whether the potential operational benefits outweigh the

[7] Office of Naval Research, "Navy Leaders Announce Plans for Deploying Cost-Saving Laser Technology," April 8, 2013, http://www.navy.mil/submit/display.asp?story_id=73234.

real and legitimate potential costs outlined above necessitates further capability development, albeit in a very controlled context.

To that end, this study makes two recommendations:

1. To alleviate ambiguity about the permissibility of potential operational and tactical cyber use, the OSD should affirmatively state that there are no *de jure* constraints that differ from any other type of attack capability.

2. To better inform determinations about technical feasibility, the ability to reliably adjudicate intelligence concerns, and explore potential models for providing a broader set of capabilities, OSD should develop a coordinated plan across the Department of Defense for experimentation and exercises that explore operational and tactical cyber use. This plan should ensure that, collectively, the activities will produce insights into whether and how such capabilities might be employed more broadly in the future. To best advance development, OSD should clearly identify the desired effects, against current military problems with targets that are deemed compliant with the Law of Armed Conflict. The military services should then have the freedom to develop their own approaches for how best to deliver those effects. This type of "top-directed, bottom-executed" approach will ensure that the resulting insights are relevant to both policymakers and to the forces that might employ cyber tools going forward.

Should such experimentation occur, it would inform many follow-on activities. These would include how best to integrate cyber with other modes of providing fires, architectures for establishing cyber JOAs, and the development of data-driven cost curves to inform future resource allocation, to name just a few. All are necessary steps in the continuing evolution of cyber capabilities, capabilities that may be uniquely well suited to meeting the strategic challenges that confront the nation.

Some may argue that an experimentation plan, at least implicitly, already exists, as reflected in the reality that each of the services has developed various tools, operations have been approved and executed, and some cyber exercises are being conducted. But to date, these activities remain tightly controlled. If offensive cyber capabilities are ever to be utilized more fully by general purpose or traditional commanders, further elaboration of how this transition will occur is needed, at least in the view of representatives from each of the military services with whom the study team has interacted. As noted above, a DoD-wide plan could include, on a deliberate timeline, aspects of the following: incorporation of offensive cyber capabilities into routine service exercise programs such as those conducted at 29 Palms, the National Training Center, Nellis Air Force Base, and various naval certification exercises;[8] the development of procedures enable the appropriate use of highly classified tools and/or the development of additional tools for use by "general purpose" commanders; and coordinated modeling and simulation efforts aimed at assessing predicted effects of cyber tools designed to address the full range of service-specific tactical and operational targets, desired effects, and conditions.

These actions are not intended to presuppose an eventual decision about offensive cyber use at lower levels, but instead to set the conditions so that such a decision, in the future, can be more fully informed. As one workshop participant noted, adversaries are at least to some degree already pursuing (and using) some of these capabilities. If the United States wishes to consider doing so in the future, it will almost certainly require more information than we have now. While much progress has been made, the value of the parts of the offensive cyber table that relate most directly to operational and tactical level commanders is still a matter of vigorous debate. To continue to move ahead, as General Cartwright exhorted, we need to get out there and experiment.

[8] These would not be limited to "cyber-focused" exercises, but would be incorporated into exercises that stress integrated operations and combined arms.

About the Author

Maren Leed is senior adviser with the Harold Brown Chair in Defense Policy Studies at CSIS, where she works on a variety of defense-related issues. From 2011 to 2012, she served as senior adviser to the chief of staff of the U.S. Army. From 2009 to 2011, she was a senior fellow and director of the New Defense Approaches Project at CSIS, where she led projects on topics as diverse as military personnel costs, the future of ground forces, reforming the military personnel system, strategic forecasting, organizing for electromagnetic spectrum control, amphibious capabilities' contributions to deterrence and shaping missions, and service cultures. She also supported the U.S. Department of Defense (DOD) inquiry into the shootings at Fort Hood. She previously served as an analyst at the RAND Corporation, where she led projects relating to intelligence, surveillance, and reconnaissance (ISR) and countering improvised explosive devices (IEDs). From 2005 to 2008, she was assigned as a special assistant to the vice chairman of the Joint Chiefs of Staff and was responsible for a range of issues including IEDs, ISR, cyber operations, biometrics, rapid acquisition, and Iraq policy. From 2001 to 2005, she was a professional staff member on the Senate Armed Services Committee, where she handled the operation and maintenance accounts and conducted oversight of military readiness, training, logistics, and maintenance for committee members. She was an analyst in the Economic and Manpower Analysis Division of the Office of Program Analysis and Evaluation in the Office of the Secretary of Defense from 2000 to 2001, where she conducted macroeconomic analyses relating to military manpower and coordinated DOD performance contracts with defense agencies. She was a doctoral fellow at RAND from 1995 to 1999, analyzing military manpower issues, training for operations other than war, and leader development, and providing strategic planning support for the military and private-sector organizations. Dr. Leed received her A.B. in political science from Occidental College and her Ph.D. in quantitative policy analysis from the RAND Graduate School.

North Avenue, Atlanta, GA 30332
www.gtri.gatech.edu/

1800 K Street NW | Washington DC 20006
t. (202) 887-0200 | f. (202) 775-3199 | www.csis.org