The American Foreign Policy Council
Defense Technology Program Brief

January 2016 Washington, D.C. No. 14

Military Cyber Operations: A Primer

By Trey Herr and Drew Herrick

Briefing Highlights

Instead of "cyber war," MCO focuses on cyber conflict or what we call "cyber-enabled warfare," in which cyber capabilities are deployed in conjunction with conventional forces.

• • •

Hidden vulnerabilities in commercial off-the-shelf (COTS) software retain value for future military use, but also risk discovery by malicious parties…This impacts military and government agencies using COTS solutions as those same unpatched vulnerabilities leave .mil and .gov networks open to attack.

• • •

An important consideration is the role of precedent, where the use of novel techniques, especially in offense, can establish a new baseline for permissible (or tolerable) behavior among allies and opponents.

• • •

On average, cyber interoperability with allies is unlikely to be a high priority, due to obvious concerns over information sensitivity and the high stakes involved. Alliance cooperation can still take place within the larger joint operations framework

• • •

Militaries are reluctant to either promote or contest any particular rule or norm absent an understanding of its operational impact…If international rules and norms are adopted, how can states ensure that signatories are properly following the agreements?

BACKGROUND

Cyber Kinetic War: When Code Hurts

Today, more than 100 of the world's militaries have some sort of organization in place for cyber warfare. These organizations' size, scale, training and budgets all differ, but they all share the same goals: In the words of the U.S. Air Force, the purpose of cyber warfare is "to destroy, deny, degrade, disrupt, [and] deceive," while at the same time "defending" against the enemy's use of cyberspace for the very same purpose. Among military planners, it's known as the "Five D's plus One."

Interest in these kinds of operations is exploding within the U.S. military. There is also a broader debate beginning in various militaries as to how such units should be organized. This very same shift is underway in China. Spending on cyber warfare became a "top funding priority," up a reported 20 percent in the last year alone, and a host of new units were created with the responsibility of "preparing attacks on enemy computer networks."

We won't just see the stealing information or revealing information, but the blocking of information or changing information. And, as such, we will see cyber operations shift from the field of espionage to having actual direct effects on the flow of battle.

For example, one of the key advantages of the U.S. military has been its global network of command and control, with the Global Positioning System being a key part of the architecture that allows forces to operate with incredible precision. But that dependence points to a key aspect to target. In 2010, a software glitch knocked 10,000 military GPS receivers offline for more than two weeks.

Maybe worse is using access to a system not to steal or block information, but to change it. In 2007, through a mix of cyber and electronic means, Israel was able to deceive Syrian air defenses into thinking that it was a regular night like any other, when in fact seven Israeli F-15s were flying overhead on their way to drop bombs on a suspected nuclear site.

Changing information might not just allow physical damage to happen through other means, but even directly cause it. Stuxnet was a piece of software code, allegedly created by U.S. and Israeli intelligence, that was used to sabotage Iranian nuclear research facilities. It did so by instructing the industrial control systems literally to damage themselves, all the while telling their human operators that everything was functioning well. Or, we might see "battles of persuasion," where one's own weapons are instructed to something contrary to owner's intent. Such changes are not just something that can be caused by outside software sneaking in, but might also come through a hardware hack, where the flaws are literally baked into the systems themselves. The result for the targets would be an experience akin to the first episode of Battlestar Galactica, where the good guys' aircraft just stopped working all at the same moment, opening them up to a devastating attack.

Background information by Peter W. Singer, co-author of *Cybersecurity and Cyberwar: What Everyone Needs to Know.*

What is the role of cybersecurity in the conduct of war and ongoing security operations? Policymakers, academics, and journalists often think of cybersecurity as a single domain problem. That is to say, they view cyber operations as taking place solely within its own domain—one that is separate from land, sea, air or space.[1] This perspective, however, overlooks the fact that computer systems and networks pervade society and the physical environment, and are present to some degree in all physical environs and across the three levels of war (strategic, operational, and tactical). Modern militaries employ forces in a "joint" manner, combining the specific platforms and technologies of different services to achieve a more effective force. National security policymakers should similarly see both kinetic and cyber capabilities as part of a broad set of tools available to achieve their objectives. Thinking of cybersecurity as a limited or separate space, wholly distinct from the other domains of conflict, limits the potential for understanding its strategic utility.

The term Military Cyber Operations (MCO) covers the acquisition and use of cyber capabilities in the strategic, operational, and tactical realms by states and non-state actors. It encompasses a broad array of defensive efforts and offensive missions, both on and off the battlefield. This topic cluster focuses on the development of capabilities, their deployment to defend the United States and allied forces, their use in targeting hostile networks, key relevant legal and diplomatic issues, the budgeting and procurement process involved in each of these areas, and, importantly, the recruitment and training of uniformed personnel to carry out these missions across all five services in the U.S. military. Notably, only a small percentage of cyber operations are offensive and destructive in nature. While incidents like Stuxnet (the malicious software deployed against Iran's nuclear program) certainly grab headlines, the day-to-day exercise of securing organizations against attack represents a far more common activity.

An array of issues affects the military's ability to train, equip, and employ cyber capabilities within both offensive and defensive missions alongside conventional forces. Effective exploitation demands newly capable talent in uniform and trained to use the same targeting and planning tools as their kinetic counterparts, but with an understanding of spectrum and network-based activity. Doctrine on everything from the use of force to passive reconnaissance has to be developed in line with the needs and capabilities of individual services, and bounded by a coherent legal framework. In addition to understanding how to properly deploy these capabilities, policymakers must also grapple with how to oversee technology procurement and maintenance as part of a range of joint capabilities. This brief aims to provide a useful overview of Military Cyber Operations (MCO), including acquisition, defense, offense, and the rules and norms that govern these activities.

Explaining Military Cyber Operations

Military Cyber Operations (MCO) is an umbrella term for the acquisition and use of cyber capabilities at the strategic, operational, and tactical levels of conflict.[2] MCO is *not* the same as "cyber war." Cyber war, as usually articulated, focuses on two (or more) combatants exclusively deploying malicious cyber capabilities against the other side's systems, resulting in death and destruction, in order to achieve a set of explicit political goals. This formulation, however, ignores both existing U.S. military doctrine and the manner in which modern forces actually deploy such capabilities.[3] In fact, there are potentially good reasons to think that cyber war, when properly defined, won't actually take place[4] or may constitute an ineffective

***Trey Herr** is a senior research associate at the Cyber Security Policy and Research Institute and non-resident fellow with the Cybersecurity Initiative at New America. Together with Rich Harrison (AFPC), he is the creator of this briefing series. His work focuses on the relationship between state power and information security including trends in state developed malicious software, the structure of criminal markets for malware, and the regulatory environment for "cyber weapons." **Drew Herrick** is a Political Science PhD Candidate specializing in international relations and research methods at George Washington University. He is also a RAND researcher and a Nonresident Fellow in the International Security Program at New America. He studies issues relating to the intersection of international security and technology, especially strategic counter-norm activity, offensive social media operations, and the military value of cyber capabilities.*

policy tool.[5]

Instead of "cyber war," MCO focuses on cyber conflict[6] or what we call "cyber-enabled warfare," in which cyber capabilities are deployed in conjunction with conventional forces. MCO is further broken up into three categories: Department of Defense (DoD) information network operations (DoDIN), defensive cyberspace operations (DCO), and offensive cyberspace operations (OCO).[7] DoDIN deals with routine information assurance,[8] such as secure network configuration, systems administration, patching, and educating individual users. DCO focuses on both passive and active defense measures, and usually entails a higher degree of expertise than DODIN activities (including detecting, analyzing, and mitigating active threats). OCO, although involving a comparatively small sliver of both personnel and resources, is perhaps most technically challenging aspect of MCO, and involves deploying cyber capabilities to disrupt, deny, degrade, or destroy another actor's systems. Here, the difference usually focuses on whether the operation is taking place on friendly systems, neutral systems, or on an adversary's systems.

MCO also includes Intelligence, Surveillance and Reconnaissance (Cyber ISR) activities and Operational Preparation of the Environment (Cyber OPE).[9] Cyber-enabled ISR focuses on gathering information on a specific adversary's systems, including their hard/software configurations, personnel, and operational security. This information is critical for effective targeting, operational planning, and "weaponeering" capabilities to achieve their desired effects. Cyber OPE, for its part, focuses on access to a target system, and on the means of preparing it for the specific operation. Access to a target's system is usually restricted by default, so advanced and up-to-date working knowledge of the target system is needed to ensure present and future access.[10]

In the United States, MCO is distinct from Information Operations (IO), Information War (IW) or even Military Information Support Operations (MISO) (formerly known as PSYOP).[11] Information Operations focus on attacking an adversary's human or automated decision-making, as well as on bolstering that of friendly forces. They focus on diverse areas such as military deception, operations security, and public affairs. In practice, Information Operations often include elements of cyber operations, but are broader, encompassing messaging and persuasive efforts governed by separate doctrine and employing a different set of personnel.[12] The degree of integration between Cyber, Electronic Warfare (EW), and IO varies among the different U.S. military services. In fact, there is an ongoing set of policy discussions centered on whether there should be deeper doctrinal and organizational integration between Cyber, EW, and IO to facilitate better asset coordination and improve military effectiveness.[13] Importantly, in other countries, such as Russia and China, Information Operations are significantly more integrated with MCO and EW.[14]

Buy and Build

How does the military build, buy, and train for these sorts of operations? Part of the challenge in acquiring a capability is integrating it into an existing concept of operations. Simply put, how a service wants to fight shapes the way it buys equipment and trains personnel.

Developing Capabilities

Development is the process of writing code to create capabilities. Our means for understanding capabilities is the PrEP framework, which defines malicious software as the combination of a propagation method, exploits, and a payload designed to create effects.[15] The propagation method is any means of transporting code from its origin to a target, such as a portable flash drive or the spear phishing emails that target public and private organizations every day. Exploits are small pieces of code written to take advantage of vulnerabilities in software; small features or flaws that allow a third party to gain access and take control of a computer. The payload is the purpose: code written to achieve some desired end, such as the deletion of data or the creation of physical destruction.

The three components work in concert, but have substantially different roles. The propagation method spreads the malicious tool, while the payload is written to create some effect on a computer system. The payload of a piece of malicious software executes on a computer system in order to create some effect, such as the alteration of data, the creation of a "backdoor" for future access, or the damage of hardware. These actions manipulate the intended function of an information system to achieve the attacker's desired effects. The term cyber weapon, though widely misused, should cover only those tools with payloads capable of generating destructive effects.[16] Exploits involved in hacking a common piece of software like Internet Explorer may open the door for a payload, but they do not directly achieve anything malicious. Without one or several exploits, a payload would almost never be able to execute on a target system, so exploits are critical to develop effective offensive capabilities and play a central role in assessing an organization's defenses.

Vulnerability Acquisition

Acquiring and integrating vulnerabilities into these cyber tools plays a central role in their development. It also creates a serious quandary for the policymaker. On the one hand, many of the targets for offensive action are foreign hard- and software systems. As a result, locating a vulnerability and building an exploit for them will not directly impact U.S. citizens. Attacking some of these targets, however, requires compromising common commercial software and less specialized civilian hardware, like routers.[17] Developing vulnerabilities for software made by American vendors like Google or Microsoft requires locating security holes in this software and keeping the information secret from these same firms, thus denying them the opportunity to fix the bugs and improve security for average users. This secrecy is necessary; a target's vulnerability, once patched, is no longer useful. However, this state of affairs engenders a debate about the cost of preserving a capability versus allowing vendors to improve the security of software commonly used by U.S. citizens.

Exploits are a commodity-like component, bought and sold actively on underground markets on the web and between private companies, defense contractors, and governments. Because an exploit targets a vulnerability in a particular piece of software—for example, Internet Explorer as opposed to Google's Chrome browser—developing a good one can yield tremendous value, with quoted prices ranging into the hundreds of thousands of dollars.[18] Increasingly, companies such as VUPEN and a sizable collection of freelancers are selling newly discovered vulnerabilities and exploits to governments and non-state actors rather than the original software vendors themselves.[19]

This represents a problem, because information security starts with secure software. The ability for vendors to discover vulnerabilities and patch them is an important part of securing software. Hidden vulnerabilities retain value for future military use, but also risk discovery by malicious parties who may deploy them against the United States. Vendors are left unaware of the flaws, and thus are unable to secure their code. This also impacts military and government users, because the use of commercial off-the-shelf (COTS) solutions like Amazon web services and the Microsoft operating system mean those same unpatched vulnerabilities leave .mil and .gov networks open to attack.

Creating a legal framework for the acquisition of these capabilities requires balancing security against capability. So far, this debate has taken place largely in the classified realm, with interagency wrangling overseen initially by the National Security Agency and now the National Security Council.[20] Problematically, this approach emphasizes selective disclosure on a case-by-case basis, rather than the establishment of broad and consistent standards that can build in existing research, procurement law, and oversight mechanisms.

Personnel

The individual military services have the responsibility to organize, train, and equip forces for operational use by the unified combatant commands.[21] Created in part as a result of the Goldwater-Nichols reforms passed in 1986, this distribution of responsibility is intended to centralize the personnel training and retention pipeline squarely in the services and clarify the responsibility for planning and executing missions.[22] How each of the services defines their missions, however, can have a sizable impact on the type of roles they organize and personnel capabilities they seek to develop. While there are common challenges across each—namely, those of assuring the integrity of information systems and conducting defensive cyber operations—the offensive missions and general concept of operations differ between the services. Integrating officers, warrant officers, and enlisted personnel trained in each of these respective cultures can pose a challenge to the unified combatant commands, and to the dedicated U.S. Cyber Command (CYBERCOM), currently part of U.S. Strategic Command (STRATCOM), which is responsible for much of the cyber mission set.[23]

Another challenge is integrating existing occupational specialties and service branches that train towards different responsibilities. For example, the Army recently created a dedicated Cyber Branch—its first new specialized branch since the establishment of the Special Forces in the 1980s.[24] The goal of this effort is to integrate individuals spread between the Signal and Intelligence branches, as well as to centralize the training and certification pipeline for cyber operations.[25] Previously, the Army had split its specialties between network defense and network offense; defensive enlisted personnel were classed in the Signals branch under 25D (Cyber Network Defender), while Military Intelligence housed 35Q, the cryptologic network warfare specialty.[26] The demand for trained personnel remains high, as the service components supporting CYBERCOM's Cyber Mission Forces remain undermanned. But the relevant pipelines are coming online slowly; the Army Cyber School in Fort Gordon Georgia graduated its first class of officers only in August 2015.[27]

Nonetheless, there is a personnel shortfall in existing units, and it will be difficult to train individuals to a high degree and then retain them against highly competitive private sector salaries. Two mitigating factors exist, however. First, not all roles are created equal—many defensive and offensive personnel act in a supporting capacity, especially in managing the configuration and security maintenance of networked systems. This means that the level of training and specialization required is lower than for autonomous operators developing and deploying capabilities organically within maneuver units on the battlefield or within the Cyber Mission Forces. The variety of skill sets and training requirements will benefit from increased standardization and clarity across the length and breadth of the Defense Department.[28] Second, and perhaps equally important, is that even where trained personnel return to the private sector, the skills and experience they bring with them could help private sector firms enhance their security and potentially avoid some of the challenges facing the public sector.

Spectrum of Use

As briefly discussed above, military cyber operations pervade all three levels of war (strategic, operational, and tactical).[29] At the *strategic level*, the motivating question is how to deploy military forces to achieve the goals for particular national objectives. The *operational level* examines how military force is able to achieve the goals of a particular military campaign. Finally, the *tactical level* focuses on the conduct of individual engagements within a campaign. In practice, the difference comes down to a question of scale and what type of forces are involved at any given point. In terms of military cyber operations, each level of war presents a different set of relevant targets and tradeoffs, and requires varying degrees of expertise. Each level also presents distinct challenges to operational planners, personnel engaged at the point of attack, and national policymakers.

Strategic

Most of the conversation about military cyber operations tends to focus on the strategic level, where the national assets and capabilities of the military and associated intelligence organizations come to the fore. The primary purpose is to create effects that advance national priorities, above the objectives of a particular battlefield or campaign. Targets at the strategic level may include civilian infrastructure with national security implications as well as military hardware, creating both digital and physical destructive effects. The scope of potential targets is global, and the larger political context where defensive and offensive cyber operations (DCO and OCO, respectively) take place could impact all countries, either directly or by implication. An important consideration is the role of precedent, where the use of novel techniques, especially in offense, can establish a new baseline for permissible (or tolerable) behavior among allies and opponents.

At this level, capabilities and the chain of command associated with their employment are closely interlinked by virtue of physical proximity—thus, the major headquarters for both CYBERCOM and the National Security Agency are located just outside Washington, DC. However, there are some important legal separations, based largely on the types of organization involved. The military typically distinguishes between main elements and supporting ones; that is, the force intended to execute an operation on the target and another providing support. Operational responsibilities can thus end up split between multiple organizations. This can lead to resource imbalance, where the group that owns the expertise dictates the terms and focus of an operation.[30] It also creates a complicated set of turf wars which have evolved from "the DoD's communications and intelligence 'tribes,' each [of whom] has developed legacy capabilities and counter-capabilities largely independent of other tribes' efforts."[31]

There are legal distinctions as well. Title 10 of the *U.S. Code* covers all three military departments (as well as the associated services) and their operations, both in peacetime and during war. By contrast, the intelligence community and its collection activities, as well as all covert action, fall under Title 50. This segmentation poses a challenge, because tools used on hostile networks for intelligence gathering can also be employed as a platform to conduct offensive operations. Similarly, espionage activities may also be used to support ongoing defensive and offensive operations, including providing information to attribute the source of compromise or target a response.

At one point, cyber operations may have been considered the domain of the intelligence community, where Title 50 requires a presidential finding prior to the initiation of a covert action.[32] The 2011 *National Defense Authorization Act* (NDAA), however, included a provision (Section 954) which granted the Defense Department authority to conduct offensive operations, "…to defend our Nation, Allies and interests…" upon the direction of the President.[33] Several scholars have interpreted this change as providing authorization for offensive activities by the Defense Department without the explicit acknowledgement of U.S. involvement—a definition close to that of covert action. The scope of authorization in this capacity may have shifted as well, allowing broader execution orders (EXORDs) that encompass a range of potential incidents and responses, obviating the need to obtain a presidential authorization for every particular operation.[34]

Operational

At the operational level, military forces may focus on an adversary's integrated air defense systems, logistics train, or supporting intelligence collection and analysis chain.[35] In practice, much of the deployment of capabilities happens at higher echelons that are not in the direct area of the campaign. Relevant parties are able to communicate easily, and friendly systems can be properly secured and supported. This stands in contrast to activities at the tactical level, where operators are often forward deployed and require more mobile capability and flexible deployment options.

The importance of joint operations rings out at the operational level. For example, in the case of air defenses, offensive cyber capabilities may be deployed to temporarily disrupt an adversary's systems in order to allow friendly sorties in the area in support of ground forces, humanitarian supply drops, or even for longer-range cruise missile strikes. Conversely, a cyber capability can be used to temporarily disrupt an adversary's air defenses so more conventional airstrikes can be conducted on the relevant facilities without concern over retaliatory fire.

A key policy consideration is the extent of cooperation with allied forces that may possess different organizational structures and levels of capability. As has been reported, the U.S. military does not habitually share offensive capabilities with military allies.[36] In some cases, however, sharing agreements could entail a limited exchange of threat detection or intelligence information.[37] On average, cyber interoperability with allies is unlikely to be a high priority, due to obvious concerns over information sensitivity and the high stakes involved. Alliance cooperation can still take place within the larger joint operations framework, however. For example, U.S. cyber operators may unilaterally deploy a specific capability while allies separately deploy their own or, more likely, use conventional forces in a supporting role.

Tactical

At the tactical level, military forces are focusing on smaller force configurations and must consider immediate environmental variables, like the shape and structure of a city and its associated electrical grid and civilian wireless networks. Vulnerabilities exist in potentially new targets like weapon systems and the larger internet of things, like vehicles,[38] as well as in traditional assets like communications systems.[39] The degree of mobility involved at the tactical level, combined with the smaller target area, presents several different battlefield issues. First, since operators are working in an active combat zone, they are vulnerable to counter fire. Second, there are, on average, higher time constraints in combat, since cyber effects have to be delivered in real time during an ongoing engagement. Combined with moving targets and varying distances, this may shrink the window of both time and space in which a particular vulnerability is effective. Finally, the particular nature of the environment may also make tailoring and testing cyber capabilities more difficult.

On the other hand, tactical cyber operations can have a few important advantages. Adversaries may not be attuned to their poor security and hardware vulnerabilities at close distances. Consequently, the adversary may mistakenly believe that the tactical level is comparatively less vulnerable than the operational or strategic environment. At the tactical level, close proximity to the target also opens up the opportunity for not just network but spectrum attacks as well. Traditionally, cyber capabilities are thought of as network centric only, accessing an adversary's system and causing an effect through networked information systems. However, at the tactical level, operators can exploit the electromagnetic spectrum as a means to access, disrupt, or degrade a target's systems like radios or power generation equipment.[40] Friendly forces can even use the electronic spectrum as a delivery mechanism for a cyber capability.[41] Finally, close proximity to the battlefield also enables forces to more reliably gauge the effectiveness of a capability on a target.

Setting the Rules

Military Cyber Operations (MCO) is a relatively new strategic arena, and therefore the rules and norms that exist are less developed than in other military and technological contexts, and subject to greater debate between domestic and international actors. This final section addresses several norms that may potentially govern the strategic, operational, and tactical use of offensive cyber capabilities. The problem of MCO's "newness" is made even more difficult by the absence of large-scale use of cyber capabilities in conflict—at least to date. This is certainly a positive historical development, but one that exacerbates the lack of precedent, since militaries are reluctant to either promote or contest any particular rule or norm absent an understanding of its operational impact. A separate but related issue is the enforcement question: if international rules and norms are adopted, how can states ensure that signatories are properly following the agreements? Nevertheless, there are a few areas where ideas have begun to converge.

The UN Group of Governmental Experts

The United Nations Group of Governmental Experts on Information Security (GGE) agreed in July 2015 to a consensus document laying out recommendations for state activity in cyberspace.[42] The 2015 paper reiterates the importance of confidence building measures, but goes further than previous drafts by outlining guidelines for military cyber operations and critical infrastructure protection.[43] Specifically, states should respond to requests for support and refrain from engaging in activity that intentionally damages or impairs critical infrastructure or computer emergency response teams (CERTs). The report goes even further toward applying international legal principles (such as necessity and proportionality) to cyber activity. In all likelihood, a 2016 or 2017 successor group will be formed.

The U.S. Department of Defense (DoD) Law of War Manual

The DoD's Law of War Manual[44] reinforces previous claims that existing laws of war are generally applicable to cyber operations, but leaves open the possibility of changes in the future, for example by redefining the types of tools classified as weapons. On the issue of a cyber "act of war," the manual argues that cyber incidents are not necessarily armed attacks for the purposes of triggering a State's right to self-defense. Cyber incidents are also "not necessarily 'attacks' for the purposes of applying rules on the conduct of operations during hostilities."[45] As well, the Manual does not obligate neutral parties to refrain from relaying an actor's information or data through their own cybersecurity infrastructure. Through these and related claims, the Manual largely codifies existing U.S. positions.

The Tallinn Manual and the Laws of Armed Conflict

The Tallinn Manual on the International Law Applicable to Cyber Warfare[46] is the product of a three-year NATO Cooperative Cyber Defense Center of Excellence effort to offer a summary of international law as it applies to cyber conflict. This manual outlines 95 rules that govern international cyber conflict, addressing issues such as sovereignty, state responsibility, the conditions for the onset of war, international humanitarian law, and the law of neutrality. Importantly, the Tallinn Manual focuses on incidents that occur as the use of force and therefore does not directly address issues of cyber crime or espionage. The Tallinn Manual's key point is that cyber conflict or "cyber warfare" is governed by existing international law, the same international rules that concern other forms of conflict including relevant portions of the UN charter, The Hague Convention of 1899, and the Geneva Convention of 1949.[47]

Conclusion

Military Cyber Operations (MCO) cover the acquisition and use of cyber capabilities at the strategic, operational, and tactical levels of conflict. MCO is properly understood as part of a combined arms approach to warfighting that is codified in the military doctrines of several States. This casts doubt on the notion of cybersecurity as a single domain issue, and mitigates against the likelihood of a domain-specific "cyber war." While offensive issues dominate doctrinal and legal discussions, defensive missions have proven to be more frequent and resource intensive challenges to the military and related organizations. There is also an unsettled set of procurement, personnel, and strategic questions that impact the day-to-day activities of CYBERCOM and the military services—a fact which may undermine U.S. operational effectiveness over time. While the norms of behavior governing MCO are still far from settled, there is at least some consensus over the application of existing international rules, like proportionality and restraint, especially in reference to civilian targets. The pace of technological change is rapid, but the selection of organizational, planning, and oversight challenges discussed in this brief remain persistent and, in some cases, incredibly ordinary. How policy adapts to fit and fulfill the needs of soldiers employing these capabilities on and off the battlefield will help shape the future of the force and impact national security decisionmaking for decades to come.

Endnotes

1)"War in the Fifth Domain." The Economist, July 1, 2010, http://www.economist.com/node/16478792.

2) Trey Herr and Allan A. Friedman. "Redefining Cybersecurity." American Foreign Policy Council Defense Technology Program Brief no. 8 (2015), http://papers.ssrn.com/sol3/Papers.cfm?abstract_id=2558265.

3) For example, consider Russian forces in Georgia or Ukraine. Similarly, consider U.S. cyber operations in Iraq or plans for their use in Libya. Eric Schmitt and Thom Shanker, "U.S. Debated Cyberwarfare Against Libya," New York Times, October 17, 2011, http://www.nytimes.com/2011/10/18/world/africa/cyber-warfare-against-libya-was-debated-by-us.html.

4) Thomas Rid, Cyber War Will Not Take Place, first edition (New York: Oxford University Press, 2013).

5) Erik Gartzke, "The Myth of Cyberwar: Bringing War in Cyberspace Back Down to Earth," International Security 38, no. 2 (October 1, 2013), 41–73.

6) Chris Demchak, "Cybered Conflict vs. Cyber War." New Atlanticist, October 20, 2015, http://www.atlanticcouncil.org/blogs/new-atlanticist/cybered-conflict-vs-cyber-war.

7) JP 3-12(R), Cyberspace Operations, February 5, 2013

8) Trey Herr and Eric Ormes, " Understanding Information Assurance," http://ssrn.com/abstract=2589724

9) JP 3-12(R), Cyberspace Operations, 05 February 2013

10) Leed, Maren. "Offensive Cyber Capabilities at the Operational Level." CSIS. September 2013. http://csis.org/files/publication/130916_Leed_OffensiveCyberCapabilities_Web.pdf

11) Paul, Chris. Information Operations - Doctrine and Practice: A Reference Handbook. Westport, Conn: Praeger, 2008.

12) Paul, Chris. Information Operations - Doctrine and Practice: A Reference Handbook. Westport, Conn: Praeger, 2008.

13) http://www.cerdec.army.mil/news_and_media/Army_looks_to_blend_cyber__electronic_warfare_capabilities_on_battlefield/

14) Bejtlich, Richard. "TaoSecurity: More Russian Information Warfare." TaoSecurity, February 6, 2014. http://taosecurity.blogspot.com/2014/02/more-russian-information-warfare.html.; Jonsson, Oscar, and Robert Seely. "Russian Full-Spectrum Conflict: An Appraisal After Ukraine." The Journal of Slavic Military Studies 28, no. 1 (January 2, 2015): 1–22. doi:10.1080/13518046.2015.998118.; Anand, Vinod. "Chinese Concepts and Capabilities of Information Warfare." Strategic Analysis 30, no. 4 (2006): 781–97.

15) Trey Herr, "PrEP: A Framework for Malware & Cyber Weapons," The Journal of Information Warfare 13, no. 1 (February 2014): 87–106. http://ssrn.com/abstract=2343798

16) Herr, Trey and Rosenzweig, Paul. "Cyber Weapons and Export Control: Incorporating Dual Use with the PrEP Model"Journal of National Security Law and Policy, Vol.8, No.2, (October 2015) http://dx.doi.org/10.2139/ssrn.2501789

17) https://threatpost.com/disclosed-netgear-router-vulnerability-under-attack/114960/

18) http://www.wired.com/2015/11/heres-a-spy-firms-price-list-for-secret-hacker-techniques/

19) http://www.forbes.com/sites/andygreenberg/2012/03/23/shopping-for-zero-days-an-price-list-for-hackers-secret-software-exploits/

20) http://www.wired.com/2015/06/turns-us-launched-zero-day-policy-feb-2010/

21) JP-1, http://www.dtic.mil/doctrine/new_pubs/jp1.pdf

22) https://www.usnwc.edu/getattachment/744b0f7d-4a3f-4473-8a27-c5b444c2ea27/Has-It-Worked--The-Goldwater-Nichols-Reorganizatio

23) http://www.safcioa6.af.mil/shared/media/document/AFD-140512-039.pdf

24) https://defensesystems.com/articles/2014/12/11/army-cyber-branch-new-career-field.aspx

25) http://www.armytimes.com/story/military/2015/06/15/cyber-transfer-panels-and-reclassification-actions/71060716/

26) 25D - http://www.army.mil/article/116564/ and 35Q - http://www.army.mil/article/92099/Army_opens_new_intelligence_MOS/

27) http://www.fortgordonglobe.com/news/2015-08-14/Front_Page/Cyber_School_marks_major_milestone.html

28) http://www.gao.gov/assets/320/318612.pdf

29) Biddle, Stephen PS, Political Science & Politics; Jul 2007; 40, 3; ProQuest pg. 461

30) http://sites.tufts.edu/fletcherdean/divide-and-conquer-why-dual-authority-at-the-nsa-and-cyber-command-hurts-u-s-cybersecurity/

31) 21ST Century Cyber Security: Legal Authorities and Requirements by Lieutenant Colonel Charles W. Douglass United States Air Force – US Army War College - http://handle.dtic.mil/100.2/ADA561641

32) http://repository.law.umich.edu/cgi/viewcontent.cgi?article=1081&context=mlr

33) http://www.wired.com/2011/12/internet-war-2/

34) JP 5-0 http://www.dtic.mil/doctrine/new_pubs/jp5_0.pdf

35) Biddle, Stephen PS, Political Science & Politics; Jul 2007; 40, 3; ProQuest pg. 461

36) "The Role of Offensive Cyber Operations in NATO's Collective Defense." Atlantic Council. Accessed October 30, 2015. http://www.atlanticcouncil.org/blogs/natosource/the-role-of-offensive-cyber-operations-in-nato-s-collective-defense.; Nicholson, Lt. Col. Jason B. and Lt. Col. David A. Pokrifchak. "Cyber sharing" Armed Forces Journal. (December 16, 2013)

37) "The Role of Offensive Cyber Operations in NATO's Collective Defense." Atlantic Council. Accessed October 30, 2015. http://www.atlanticcouncil.org/blogs/natosource/the-role-of-offensive-cyber-operations-in-nato-s-collective-defense.; Nicholson, Lt. Col. Jason B. and Lt. Col. David A. Pokrifchak. "Cyber sharing" Armed Forces Journal. (December 16, 2013)

38) "Demo Jeep Hack Could Have Military Implications." C4ISR & Networks. Accessed October 30, 2015. http://www.c4isrnet.com/story/military-tech/cyber/2015/07/24/vehicle-hack-could-have-military-implications/30628191/.

39) "Russia Has Complete Information Dominance in Ukraine."

Atlantic Council. Accessed October 30, 2015. http://www.atlanticcouncil.org/blogs/new-atlanticist/russia-has-complete-informational-dominance-in-ukraine.

40) Kushiyama, Kristen. "ARMY LOOKS TO BLEND CYBER, ELECTRONIC WARFARE CAPABILITIES ON BATTLEFIELD" U.S. Army, Oct. 29, 2013. http://www.cerdec.army.mil/news_and_media/Army_looks_to_blend_cyber__electronic_warfare_capabilities_on_battlefield/

41) Kushiyama, Kristen. "ARMY LOOKS TO BLEND CYBER, ELECTRONIC WARFARE CAPABILITIES ON BATTLEFIELD" U.S. Army, Oct. 29, 2013. http://www.cerdec.army.mil/news_and_media/Army_looks_to_blend_cyber__electronic_warfare_capabilities_on_battlefield/

42) United Nations. "Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security." 22 July 2015. http://www.un.org/ga/search/view_doc.asp?symbol=A/70/174; "Net Politics » The UN GGE on Cybersecurity: What Is the UN's Role?" Council on Foreign Relations - Net Politics. Accessed October 30, 2015. http://blogs.cfr.org/cyber/2015/04/15/the-un-gge-on-cybersecurity-what-is-the-uns-role/.

43) United Nations. "Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security." 22 July 2015. http://www.un.org/ga/search/view_doc.asp?symbol=A/70/174

44) U. S. Department of Defense, U.S. Department of Defense Law of War Manual, 2015.

45) Ibid.

46) Michael N. Schmitt, ed. Tallinn Manual on the International Law Applicable to Cyber Warfare. (New York: Cambridge University Press, 2013).

47) Ibid.

Defense Technology Program Brief

About The Defense Technology Program

A revolution is taking place in the nature of warfare. The proliferation of ballistic missiles and weapons of mass destruction has given rogue states and terrorist groups unprecedented access to potentially devastating capabilities, while space and cyberspace have emerged as distinct new arenas of strategic competition. The American Foreign Policy Council's (AFPC) work in these areas is aimed at helping U.S. offcials understand and respond to this new, and increasingly complex, threat environment.

For more information about the program, please contact Richard Harrison, Director of Operations and Defense Technology Programs at harrison@afpc.org.

About AFPC

For over three decades, AFPC has played an essential role in the U.S. foreign policy debate. Founded in 1982, AFPC is a 501(c)(3) non-profit organization dedicated to bringing information to those who make or influence the foreign policy of the United States and to assisting world leaders with building democracies and market economies. AFPC is widely recognized as a source of timely, insightful analysis on issues of foreign policy, and works closely with members of Congress, the Executive Branch and the policymaking community. It is staffed by noted specialists in foreign and defense policy, and serves as a valuable resource to officials in the highest levels of government.

AFPC Mission Statement

The American Foreign Policy Council seeks to advance the security and prosperity of the United States by:

- providing primary source information, as well as policy options, to persons and organizations who make or influence the national security and foreign policies of the United States;
- arranging meetings and facilitating dialogue between American Statesmen and their counterparts in other countries; and
- fostering the acceptance and development of representative institutions and free market economies throughout the world in a manner consistent with the Constitution, the national interest, and the values of the United States.

CONTACT

509 C Street NE
Washington, D.C. 20002
Telephone: 202.543.1006
Fax: 202.543.1007
www.afpc.org