Offensive Cyber *for the* Joint Force Commander

NASA Defense Meteorological Satellite Program

It's Not That Different

By ROSEMARY M. CARTER, BRENT FEICK, *and* ROY C. UNDERSANDER

Satellite view of power distribution

The instruments of battle are valuable only if one knows how to use them.

—Charles Ardant du Picq[1]

In 2008, as part of the campaign against the Republic of Georgia, Russia conducted a series of widely publicized cyber attacks. The attacks were not against purely military target sets. For 19 days, cyber warriors conducted distributed denial-of-service attacks against Georgia's Internet infrastructure and defaced public and private Web sites.[2] The initial impact was a virtual cyber-blockade against the government of Georgia that reduced the country's ability to lead internally and stifled its ability to gain international sympathy. A second-order effect was that the National Bank of Georgia shut down its Internet connections for 10 days, stopping all electronic financial transactions. The strike is one of the first publicized employments of offensive cyber as an integrated part of a military operation and demonstrates the powerful impact of these types of attacks on private sector business.[3]

The cyber domain consists of four operating areas: providing capability, protecting that capacity, exploiting within the domain, and conducting offensive operations that are also referred to as computer network attack. The areas of "provide" and "protect" are the most mature because our day-to-day information technology operations require a secure and functioning cyber domain. This article focuses instead on *offensive cyber capability*, which is the newest segment of the domain but is rapidly maturing. Unlike airpower, where development was limited to nations with significant industrial and financial resources, the cyber warfare arena is inexpensive and characterized by state and nonstate actors limited only by creativity and the Internet. Therefore, to maintain strategic capability for cyber superiority,[4] the cyber domain must be rapidly synchronized with the other warfighting domains. A full understanding of the features, capabilities, limitations, and impacts of the cyber domain may be years away, but actionable knowledge of this domain at the operational level will not be achieved as long as cyber operations remain segregated from the other warfare mission areas.

The assertion that cyber operations are different is the most common argument for

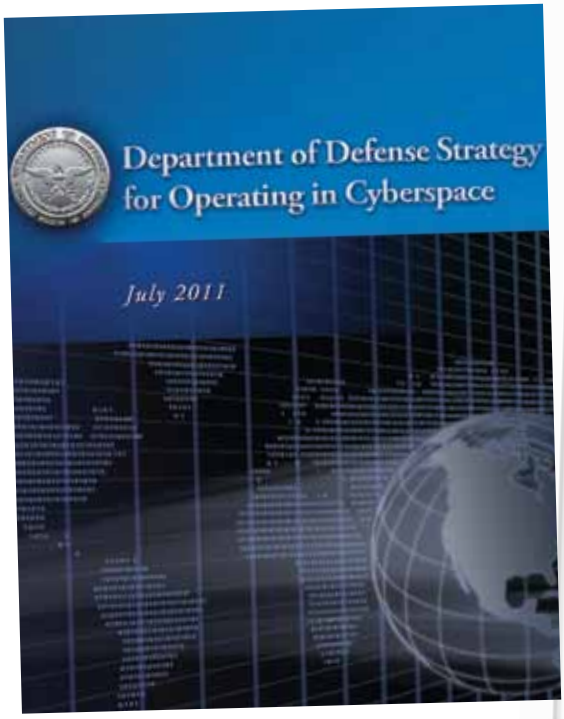
Colonel Rosemary M. Carter, USA, is a Communications Officer on the Army Staff. Colonel Brent Feick, USAF, is a Senior Policy Advisor for the Office of the Deputy Assistant Secretary of Defense for Homeland Defense and Americas' Security Affairs, Integration, and Defense Support of Civil Authorities. Captain Roy C. Undersander, USN, is the Executive Officer of Naval Air Station Jacksonville, Florida. The authors collaborated on this article while attending the Joint and Combined Warfighting School at the Joint Forces Staff College.

segregating cyber from the other domains. Cyber is different just as the solid terrain of the land domain differs from the physical structures of air and space domains. Speed of action is also different in cyber. Events occur and situations develop faster than the human mind can observe, orient, decide, and act.[5] But this is not the first time in the history of warfare that the speed of conflict has changed. The introduction of fighter aircraft and space capabilities changed the military decision calculus, yet these capabilities were not in themselves sufficient justification to segregate the domain. In fact, initial efforts to isolate space from the other domains were overcome as our understanding of the domain matured. The purpose of this article is to analyze the challenges of cyber policy, targeting, and the planning process to argue that offensive cyber is not so different from other capabilities, and that it must be fully integrated at the joint force command level to ensure unity of effort and maximize effectiveness.

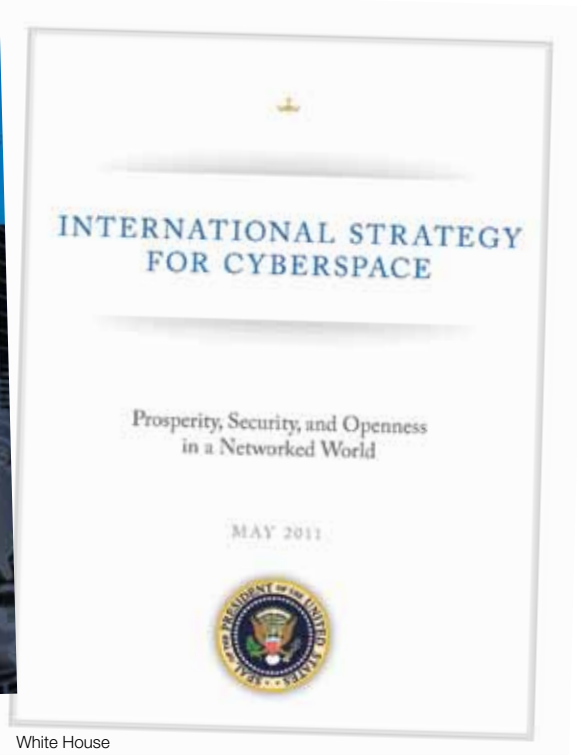
The Need for Rules

U.S. policy, authorities, and doctrine for military operations in the cyber domain are not mature. The *International Strategy for Cyberspace*[6] (May 2011) and the *Department of Defense* (DOD) *Strategy for Operating in Cyberspace*[7] (July 2011) are a start, but both documents focus almost entirely on cyber defense. While this is an important aspect, it leaves the Armed Forces in a state of flux with regard to integrating offensive capability. As is to be expected, conduct of cyber attacks is a sensitive issue. International organizations such as North Atlantic Treaty Organization (NATO) Watch advocate for a ban on offensive cyber operations altogether because the domain is so pervasive that offensive operations could quickly escalate beyond the intended virtual boundaries with devastating global impact.[8] Cyber activity is also being addressed through international anticrime channels,[9] but care must be given to provide separate and distinct definitions for acts of crime as opposed to acts of war. Without international rules, some countries have started to set precedent by their actions, demonstrating ethics that differ from ours. Standards of conduct for cyber warfare similar to those for other aspects of war are required. The United States should draft a declaratory policy that establishes lines we do not intend to cross in the cyber domain and that we expect an adversary to adhere to as well.

The U.S. Code is another source of guidance for DOD. The authorities of Title 10, The Armed Forces, and Title 50, War and National Defense, were established prior to the existence of the concept of cyberspace, so translating them to the cyber domain is extremely complex and not yet fully deconflicted. For example, under Title 10, a joint force commander is authorized to collect intelligence on an adversary for operational preparation of the environment (OPE). In the cyber domain, this task becomes mired in law because the same capability used to exploit is also used to attack, and there is no way to demonstrate intent within the effects of the task.[10] Because of the legal concerns, collection to date is done under Title 50 authorities, which severely limit military capacity and compel a centralized approach to these types of intelligence. If Service cyber components were allowed to conduct OPE on behalf of the joint force command for targeting, offensive cyber options could be much more integrated and timely. As it is, joint force planning staffs routinely lose national-level support due to higher priority tasking from the National Intelligence Priority Framework. Agencies supporting national tasking are highly skilled but have limited resources; hence, they do not have excess capacity to meet DOD requirements. Section 954 of the National Defense Authorization Act for Fiscal Year 2012[11] starts to address DOD authorities for offensive cyber operations, but it is vague enough that debates over Titles 10 and 50 will still occur. Its lack of clarity indicates that the thinking of policymakers and lawmakers is still too traditional for this newest domain.



DOD



White House

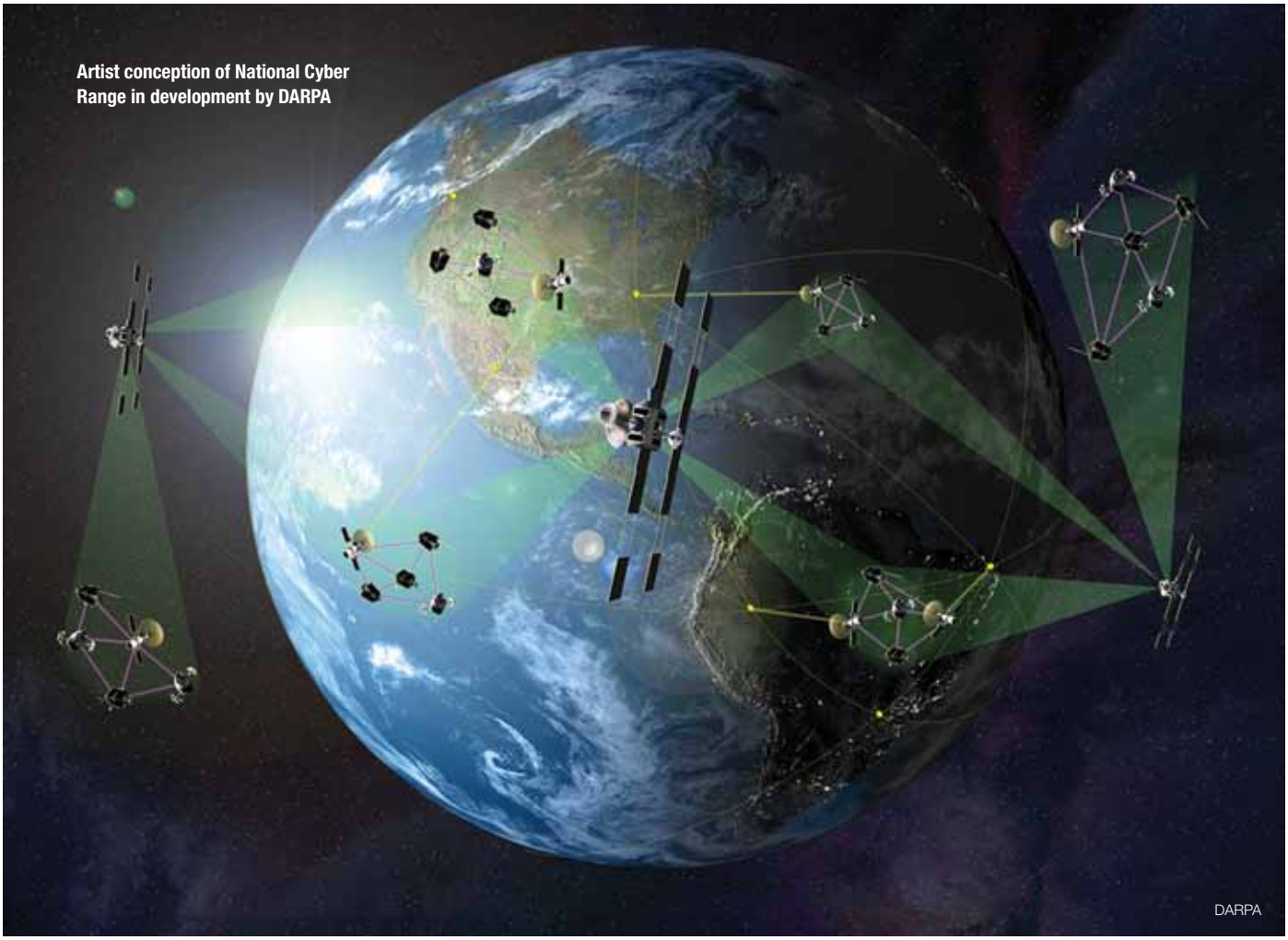
General Keith Alexander, USA, commander of U.S. Cyber Command (USCYBERCOM) and director of the National Security Agency (NSA), announced in October 2011 that DOD is currently staffing rules of engagement for the cyber domain from which his command will provide guidance to the DOD cyber force.[12] These rules of engagement are an important step, but they are not sufficient without training and rehearsals to validate and inculcate them into operational ethos.

Per DOD Directive 5100.01, the Services and combatant commands have authority to man, train, and equip cyberspace forces to enable joint force commanders to perform decisive operations.[13] Tactics, techniques, and procedures for computer network attack are maturing. What are needed now are plans to inform defense leadership and other policymakers how these capabilities integrate to achieve military and national endstates. Planning will drive understanding of current authorities and help inform recommended changes prior to a military crisis.

The Targeting Process

Military operations require effective targeting to identify objects or entities for engagement or action. To be effective, these targets must be linked to the commander's intent. In accordance with Joint Publication 3-60, *Joint Targeting*, the principles for joint targeting are focused, effects-based, interdisciplinary, and systematic.[14] The joint targeting process is cyclic and relies on target system analysis and assessments to establish functional relationships among the adversary's political, military, economic, social, informational, and infrastructural systems. The process includes both target system elements and target system components to be inclusive of all elements of the adversary's power. It is dependent on staff judge advocates to ensure that targets are in compliance with the laws of armed conflict and the rules of engagement. The targeting process is an essential component of mass and unity of effort, bringing integrated capabilities to bear during all phases of operations—shaping, deterring, seizing the initiative, dominating, stabilizing, and enabling civilian authorities.

The targeting process is as critical for the cyber domain as it is for the domains of land, sea, air, and space because we expect our adversaries to have as complex a military cyber capability as our own integrated with civilian networks. Additionally, other targets, to include manufacturing plants, logistics systems, and power generation facilities, are dependent on the cyber domain to function properly and effectively.[15] The characteristics and sophisticated intricacies of cyber make it tempting to isolate cyber targeting from the larger effort. There are some compelling arguments for this approach. First, the domain requires specialists, some of whom will never wear the uniforms of our Armed Forces. There are few cyber specialists, so the vision of a consolidated cohort of cyber targeteers ready to converge on a designated



Artist conception of National Cyber Range in development by DARPA

threat is appealing. Consolidating resources also facilitates centralized training, which is attractive in a resource-constrained environment. Finally, the shared connectivity between adversary and civilian or commercial cyber space argues for keeping cyber targeting inside of a compartmented community with a small number of personnel knowledgeable on the efforts. However, none of these arguments is sufficient to overcome the risks associated with lack of integrated targeting at the operational level. This integration is fundamental and cannot be achieved during the execution phase.

The commander and his staff must fully understand both the friendly and adversary cyber domains to the same degree they understand the other domains. As with any limited resource, the global force management system should prioritize and allocate the cyber force based on priorities and risk. Training for specialized forces will always be a challenge. However, training difficulties should not drive operational capabilities. Leaders should demand flexibility and creativity from the force providers in their training programs, not from a warfighting commander with limited access to the domain until operations are imminent. Efforts now to decentralize and optimize cyber training will also reap benefits for the operational force by establishing virtual environments that can test training, exercises, scenarios, and contingency plans.

Risk is associated with the negative second- and third-order effects of targeting an adversary's cyber space with civilian and commercial cyber activities operating in the same space. This risk is the strongest argument for integrating cyber targeting within the commander's larger targeting effort. The Georgia case study provides an example of these risks. Whether or not the cyber attackers intended for the Georgian National Bank to cease electronic transactions, the impact was the same. Unintended consequences of a limited cyber attack may impact the financial instrument of power in waves of effects generated by actual damage, perceived damages, or, as in Georgia, loss of confidence. Commanders must understand the most dangerous and most likely effects of cyber operations within their areas of responsibility. These effects must synchronize with the entire operation to protect friendly forces and the civilian population.

Joint force commanders must integrate information from the cyber domain into their joint targeting process to synchronize capabilities. This should be a two-way street, benefiting other warfare operators and, just as important for cyber operators, opening avenues of approach in other domains that otherwise would be closed in the cyber domain. While cyber information can fit into the targeting process, there are some manual manipulations that need to take place until the targeting community catches up with new policies and the supporting technology.

First, the military targeting process is geographically focused to the point that the Modernized Integrated Database, a database for all military targeting, only references targets by geographic position. This poses problems for a cyber operator who may have a virtual network as a target. The Intelligence Community is aware of this shortfall and working to make the database more flexible. Second, access to signals intelligence (SIGINT) data is too constrained. Joint planners must have access to these reports in a timely manner if they are to have a full understanding of the operational environment. SIGINT data should be pushed from NSA, not pulled. Once targets are identified, raw SIGINT may even need to be shared in order to maintain a target on the joint target list.

our country is currently more willing to drop a bomb on an adversary than break his computer

Finally, a tiered approach to identifying targets in the cyber domain must be adopted. There is an authorities question nested in this as well, but a joint force commander, with the help of all-source intelligence and a military cyber component, may produce Internet-facing targets to hold at risk. These are targets that are accessible directly from the Internet (as opposed to a closed network) and would constitute the first tier. OPE on tier one targets would not involve national intelligence assets, but would help refine questions that can focus national assets on the harder problems for the military, and thus would be the second tier. Many agencies are skeptical of the utility of Internet-facing targets, but the Georgia attack, where the known cyber targets were Internet-facing, is an example of their utility. The target list was even posted on the Internet. This discussion demonstrates that there are some differences in dealing with cyber targeting information, but in general it fits into the Joint Publication 3-60 construct.

It is incumbent upon USCYBERCOM to enable joint force staffs to fully contribute in this environment and understand the positive and negative effects of cyber operations on friendly forces, on the adversary, and on noncombatants in their area of responsibility during all aspects of targeting.

Operational Planning

Larger than the targeting process is overall planning for an operation. Today, a limited understanding of the cyber domain artificially constrains military planners. Many planners perceive that DOD does not have authority to do offensive operations in the cyber domain. However, the real issue is that the authorities are not understood or delegated down. Joint force commanders need to develop integrated plans with offensive cyber operations to help shape policy and build a norm of authorities and rules of engagement for military cyber attack, but their planners do not know the domain well enough to develop these plans. The discussion becomes circular. Civilian policymakers want to know exactly what DOD intends to do and commanders perceive that they cannot do anything because they do not have the authority.

With this, the value of the J5 Planning Directorate and deliberate plans come into play. The more fidelity joint force commanders can put into offensive cyber planning, the easier it will be to articulate potential new authorities with sufficient time to integrate them into the plan. Often, intelligence agencies will not be supportive of specific targets, citing a concern over loss of intelligence. However, this is a moot point at the planning stage, and planners should not let this, or the lack of authorities, defer their planning if the target will help meet an objective. It is better to have a plan available in times of crisis from which to have the intelligence gain/loss and legal discussions than to be caught with no options when the government is prepared to take action.

Unique features of the cyber domain have encumbered deliberate cyber planning in the past. The following generic scenario demonstrates the methodology and the unique features. A planner determines that Effect A can be met either by dropping a joint

direct attack munition on Target 1, a building, or by conducting a cyber attack on Target 2, a router. In both cases, the planner uses intelligence to link the target to the effect, determine access, pick the appropriate capability, and maintain the target in the joint target list. However, it typically takes much more intelligence preparation to develop Target 2 because our culture is so focused on geographic targets that it takes an extra level of intellectual energy to broaden the aperture. If the planner can obtain imagery of Target 1, then it is simply easier for a weaponeer to plan for a kinetic solution and hold that target at risk.

In determining access, we see the second difference. Access to Target 1 may constitute a bomber flying through or avoiding a surface-to-air missile threat. This is a well-understood problem and is addressed by the tactical force. In the case of Target 2, access must be established through the cyber domain by cyber operators, who are limited. To do this, the command requires cyber OPE or exploitation authorities as discussed. This is often where targeting in the cyber domain stops due to limited NSA resources and competition with national priorities. If Service cyber components were conducting cyber preparation of the environment under Title 10 at the joint force commander's direction, many of these issues would be resolved. As it is, these differences add up to a longer timeline to develop the target.

The third difference is the capability itself. The United States has a finite number of types of kinetic weapons to attack physical targets. Using the right combination and number of weapons, and based on experience, it is easy to quantify the level of damage that these weapons inflict, which aids in the decisionmaking process. By contrast, cyber weapons are customized for each target, which makes it difficult for decisionmakers to use experience to visualize the mode of attack and its effects. Many cyber weapons are also based on specific software versions, so if the version changes, the weapon may no longer be effective.

The fourth and most significant difference is maintaining the target, the process in which the intelligence and planning teams routinely review the intelligence and endstates to ensure that the target still meets the desired effects and nothing has changed that requires new weaponeering. This is a common task for any target on the joint target list; the difference is the volatility of the cyber target. In the case of Target 1, a planner may go 1 or 2 years between conducting maintenance. The structure of the building rarely changes and it will not move. However, Target 2 may receive a software upgrade 3 months after identification that makes the weapon developed for it obsolete. As a result, if the planner is serious about holding this target at risk, the maintenance cycle must speed up significantly.

In a *Joint Force Quarterly* article, Major General Brett Williams, USAF, stated that "our understanding of nonkinetic effects in cyberspace is immature."[16] This is a fair statement and frankly one of the biggest barriers for decisionmakers who grew up waging kinetic war. Our country is currently more willing to drop a bomb on an adversary than break his computer, which stems from two issues. First, as discussed earlier, the Nation is concerned about escalation without set standards. Second, decisionmakers are not likely to experiment with a cyber attack when lives are on the line and collateral damage is not well known. Until DOD makes the cyber attack option as tangible for a decisionmaker as dropping munitions, and can prove it will meet or exceed the effect of a kinetic option without catastrophic collateral effects, the decisionmaker will choose the kinetic option every time. To remedy this, planners must develop high-fidelity cyber attack options that are part of an integrated solution and can be tested on ranges prior to execution. This will allow the cyber community to establish a historical database to provide the confidence and statistical data required for decisionmakers to choose the nonkinetic options.

To summarize deliberate planning, the primary reason that some organizations push back on cyber planning to this level of detail is the increased level of effort to develop the target and the volatility of the target. However, if joint force commanders want to normalize cyber attack and have a reasonable expectation of successfully executing it as a part of combined fires, deliberate planning is a must. Likewise, cyber operators need to embrace this concept as well lest they become irrelevant, especially when effects cannot be brought to bear where and when they are needed for the commander.[17]

Finally, if a computer network attack is not planned for standalone delivery, the capabilities must be synchronized with the other capabilities brought to bear by the joint force commander. U.S. Strategic Command (USSTRATCOM) is responsible for or is assigned many of the nonkinetic capabilities in DOD, and its planners must work alongside joint force planners to provide the commander the most successful attack options and courses of action. This effort must include USCYBERCOM, a subunified command under USSTRATCOM that is assigned DOD cyber forces. During the integration process, joint force planners must develop an appreciation for the synergies between USCYBERCOM and the other components of USSTRATCOM. Additionally, because cyber attacks may have global implications as well as the intended regional effects, it is imperative that these options also be vetted collectively through the DOD and interagency communities. This is a coordinating task that must be completed by U.S. Strategic Command. USSTRATCOM's Joint Functional Component Command–Global Strike started a model for this, but it is immature and requires refinement and expansion. As military professionals, we have recognized the need to work closely with interagency partners to fully achieve desired endstates and ultimately the national strategy. Cyber warfare is no different and may be one of the most compelling reasons for interagency cooperation because agencies outside of DOD have authorities in the cyber domain and may have interest or even cyber attack options developed for a particular target. These tasks must be normalized into the joint interagency coordination group process to become a force multiplier for DOD.

with new fiscal constraints on the horizon, our ability to make the best use of cyber capabilities is even more important

Recommendations

This article makes the case for integrating offensive cyber at the joint force command level. The list of recommendations below is designed to generate the discussion necessary to fully develop these details. Lead agencies identified are based on the authors' understanding of current roles and responsibilities.

1. DOD must delegate proper authorities to USCYBERCOM and its components to shorten the development time of targets,

streamline cyber operational preparation of the environment, and increase throughput of the Intelligence Community.

2. USSTRATCOM/USCYBERCOM must ensure that organizational and information-sharing policies are optimized to support and include joint force planners. This includes devising methods to share raw SIGINT for timely maintenance of targets on a joint target list.

3. The Intelligence Community must update applications and procedures associated with the Modernized Integrated Database to accommodate nongeographic targets.

4. Joint force planners must incorporate high-fidelity offensive cyber plans into their deliberate plans. USCYBERCOM must facilitate this in order to train, educate, and empower joint planners. The objective is to have planners with knowledge of cyber capabilities, limitations, and basic concepts for employment.

5. DOD must establish policy that allows joint force planners to take advantage of nontraditional cyber information sources. Commercial companies are assessing many of the same problems and could be leveraged to provide critical information.

6. DOD must resource joint force commands to test offensive cyber attacks on virtual cyber ranges. The targeting community should use the test results to develop the cyber equivalent to the kinetic Joint Munitions Effects Manual, which provides a probability of damage based on target/weapon pairing.

7. DOD, in conjunction with the U.S. Government, must develop a declaratory policy for cyber warfare. It is time for the United States to lead an international dialogue on cyber warfare, perhaps modeled on the Council of Europe Convention on Cybercrime in 2001.

8. USSTRATCOM must devise a method to track nonkinetic options for global impact and incorporate these nonkinetic attack options and associated targets into the synchronizing efforts of the joint force commander's plan.

9. USCYBERCOM must standardize the interface between joint force planners and interagency partners for targeting. This may be a logical function for the Joint Inter-Agency Coordination Group, but a separate technical interagency team may be warranted. The team should be responsive to the joint force commander.

All future U.S. military operations will include the cyber domain. Cyber is where we coordinate joint functions and control weapons systems. We must operate securely across the cyber domain and commanders must protect it. Of equal importance is our ability to operate offensively within this domain to ensure dominance, restrict the offensive cyber capabilities of the adversary, and leverage cyber as a force multiplier. With new fiscal constraints on the horizon, our ability to adapt and make the best use of these cyber capabilities is even more important. Offensive cyber operations must be integrated into the joint force commander's plan, and his planning and executing staffs must understand the desired effects. As cyber domain doctrine matures, there is an opportunity to correct current deficiencies in an integrated approach through deliberate planning and the targeting cycle. This will inform U.S. policymakers and allow for new language in key policies, laws, and treaties. The United States must act quickly because the clock is ticking and the adversary is learning. Offensive cyber—it's not that different. **JFQ**

NOTES

[1] Charles Ardant du Picq, *Battle Studies: Ancient and Modern Battle*, 8th ed. (French), trans. John Greely and Robert C. Cotton (New York: Macmillan, 1920).

[2] Eneken Tikk et al., *Cyber Attacks Against Georgia: Legal Lessons Identified* (Tallin, Estonia: Cooperative Cyber Defence Centre of Excellence, November 2008), 4–5.

[3] Scott Borg and John Bumgardner, *Overview By the US-CCC of the Cyber Campaign Against Georgia in August of 2008*, A US-CCC Cyber Special Report, August 2009, available at <www.registan.net/wp-content/uploads/2009/08/US-CCU-Georgia-Cyber-Campaign-Overview.pdf>.

[4] Cyber superiority is comparable to air superiority, which is defined in Joint Publication 1-02, *Dictionary of Military and Associated Terms* (Washington, DC: The Joint Staff, as amended through November 15, 2011), as "that degree of dominance in the air battle of one force over another which permits the conduct of operations by the former and its related land, sea and air forces at a given time and place without prohibitive interference by the opposing force" (16). In the cyber domain, superiority provides the degree of dominance in cyber that permits the conduct of operations by land, sea, air, and cyber forces without prohibitive cyber interference.

[5] Colonel John Boyd, USAF, "Destruction and Creation," September 3, 1976. Boyd's concept of the OODA loop (observe, orient, decide, act) was developed and presented through a series of briefings and lectures. His paper, "Destruction and Creation," provides scientific justification for decisionmaking without describing the OODA process in detail. Several books on the life of Boyd provide additional detail on the concept and a five-slide set titled "The Essence of Winning and Losing" dated June 28, 1995, that defines the OODA loop is attributed to Boyd.

[6] *International Strategy for Cyberspace: Prosperity, Security, and Openness in a Networked World* (Washington, DC: The White House, May 2011).

[7] *Strategy for Operating in Cyberspace* (Washington, DC: Department of Defense, July 2011).

[8] Ian Davis, NATO Watch, "Ban on offensive cyber operations needed," available at <www.natowatch.org/node/463>.

[9] Convention on Cyber Crime, ETS 185, Council of Europe, November 23, 2001, available at <http://conventions.coe.int/Treaty/Commun/QueVoulezVous.asp?NT=185&CL=ENG>.

[10] Robert Chesney, "Military-Intelligence Convergence and the Law of the Title 10/Title 50 Debate," *Journal of National Security Law and Policy*, October 17, 2011; and University of Texas Law School, Public Law Research Paper, available at Social Science Research Network, available at <http://ssrn.com/abstract=1945392>.

[11] The National Defense Authorization Act for Fiscal Year 2012 was signed by President Obama on December 31, 2011. The bill is available at <http://armedservices.house.gov/index.cfm/ndaa-home>.

[12] Donna Miles, "Doctrine to Establish Rules of Engagement Against Cyber Attack," American Forces Press Service, October 20, 2011, available at <www.defense.gov/news/newsarticle.aspx?id=65739>.

[13] Department of Defense (DOD) Directive 5100.01, *Functions of the Department of Defense and Its Major Components* (Washington, DC: DOD, December 21, 2010).

[14] Joint Publication 3-60, *Joint Targeting* (Washington, DC: The Joint Staff, April 13, 2007), I-4.

[15] Benjamin Lambeth, "Airspace, Spacepower, and Cyberpower," *Joint Force Quarterly* 60 (1st Quarter 2011), 46–53.

[16] Brett Williams, "Ten Propositions regarding Cyberspace Operations," *Joint Force Quarterly* 61 (2nd Quarter 2011), 11–17.

[17] Eric Schmitt and Thom Shanker, "U.S. Debated Cyberwarfare in Attack Plan on Libya," *The New York Times*, October 7, 2011, available at <www.nytimes.com/2011/10/18/world/africa/cyber-warfare-against-libya-was-debated-by-us.html_r=1&emc=etal>.