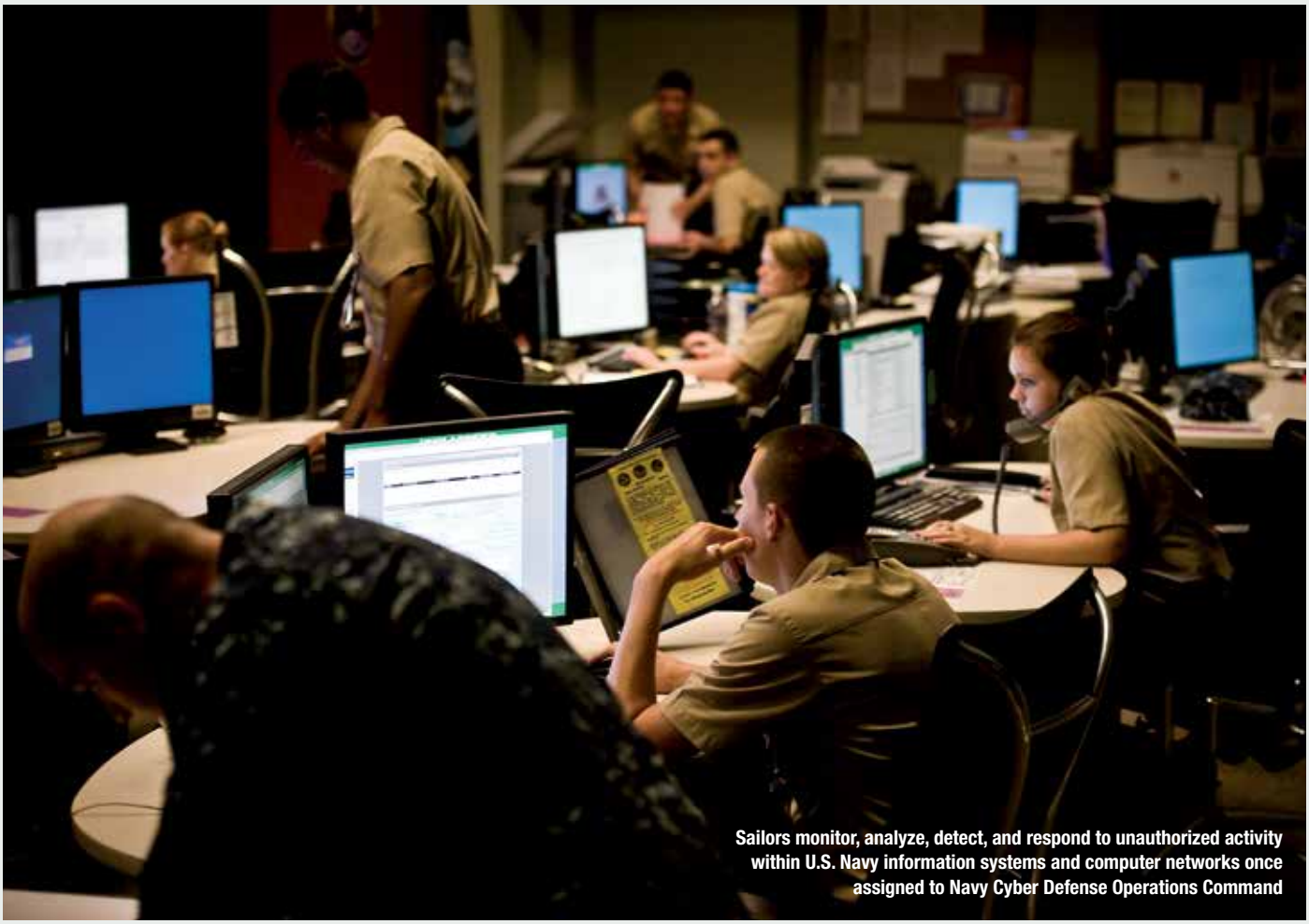


U.S. Navy (Joshua J. Wahl)

Sailors monitor, analyze, detect, and respond to unauthorized activity within U.S. Navy information systems and computer networks once assigned to Navy Cyber Defense Operations Command

Core Questions for **Cyber Attack Guidance**

By **JONATHAN C. RICE**

Colonel Jonathan C. Rice, USAF, wrote this essay while a student at the U.S. Army War College. It won the 2013 Secretary of Defense National Security Essay Competition.

Despite a decade of prolific writing, many questions about cyber power, cyber war, and cyber attack remain unresolved. In particular, national governments, including the U.S. Government, do not yet have well-formed cyber attack policies and strategies or the frameworks around which to build them.[1] Furthermore, accelerating changes in power distribution, cyber technology, and other dynamics of the strategic environment exacerbate the dearth of open, distinct, and explicit cyber attack guidance. If such well-defined guidance did exist, what questions would one reasonably expect it to answer? On what intellectual foundation should a state build its cyber attack policy and strategy? If an outsider wanted to understand an actor's strategic guidance, what clues would he look for?

Answers to these questions could—and this article argues *should*—reside in four foundational elements: contextual views, the cyber attack spectrum, balance of focus, and appropriate circumstances. How an actor approaches each of these elements fundamentally shapes the myriad details of subsequent policy and strategy. One could use a framework based on these elements as a model to think about and discuss cyber attack in a structured way, a basis for forming one's

own policy and strategy, or a tool for assessing and understanding the strategic guidance of another actor. This article first presents such a framework and then uses it to make recommendations for U.S. national guidance.[2]

Framework

The proposed cyber attack framework consists of the following four foundational elements:

- Context: To what extent does cyber attack provide a new way to do things along two dimensions—type of activities and view of the strategic environment?
- Spectrum: How broadly and in what arrangement does one consider the spectrum of cyber attack possibilities?
- Focus: What is the optimal balance of focus along the continuum of cyber attack as an enabling function, an independent capability, and a strategic attack?
- Circumstances: What are the appropriate circumstances—legal, ethical, and prudential—in which to conduct cyber attacks?

The clarity with which an actor addresses these four elements undergirds well-defined, coherent guidance. Clear conceptions do not guarantee effective policy, but they do facilitate it. Ambiguous answers will likely result in underdeveloped, inconsistent, or ineffective guidance.[3]

Contextual View. The first and most significant element addresses an actor's contextual view of cyber attack in terms of the novelty of the types of activities conducted and the strategic environment in which these occur. In its simplest expression, a cyber attack is a new way to conduct an attack; cyber provides a new set of tools to accomplish familiar tasks. This is significant. Israel's reported cyber attack against air defenses during a 2007 strike on a Syrian nuclear weapons facility provides an example. During the strike, Syrian radar screens did not show the incoming Israeli aircraft because an Israeli cyber attack had taken control of the systems, enabling the fighters to arrive undetected.[4] Other methods have been used to negate air defenses (for example, stealth aircraft and radar jamming); however, cyber attack allowed use of nonstealthy aircraft while concealing not only specific aircraft locations, but also that there was an imminent air attack at all. Cyber attack provided clear advantages, but nonetheless it performed a familiar task.

However, cyber attack also offers revolutionary capabilities. The explosion of computing power, the increasing interconnectedness of computer operations, and the integration of computers and associated networks into so many functions of modern society have led to the emergence of cyberspace as a domain unto itself.[5] Within this realm, actors can conduct activities or achieve effects not otherwise attainable.[6] This first contextual dimension captures the extent to which activities or effects represent a new kind in and of themselves, or to which they are practicable with a notably greater scope, intensity, frequency, or magnitude than what is achievable through other means.

The second dimension of the contextual view consists of the novelty and dynamic nature of the strategic environment. Four changes have occurred over the last century that collectively demand fundamentally different ways of thinking. First, the globe contains less unclaimed or internationally contested space. The end of imperial expansion, establishment of states covering the globe, development of international law, and creation of institutions to help resolve disputes have significantly reduced the amount of such territory. Hotly contested border areas, nations without states, disgruntled people within states, and undergoverned areas represent the territorial conditions and the associated nonstate actors that are most likely to produce conflict.

Second, globalization has accelerated at an exponential pace over the last few decades. Technological developments and the end of the Cold War have significantly increased global interconnectedness, especially in the international movement of information, monetary value, people, and cargo. Cyberspace has both contributed to and resulted from globalization.

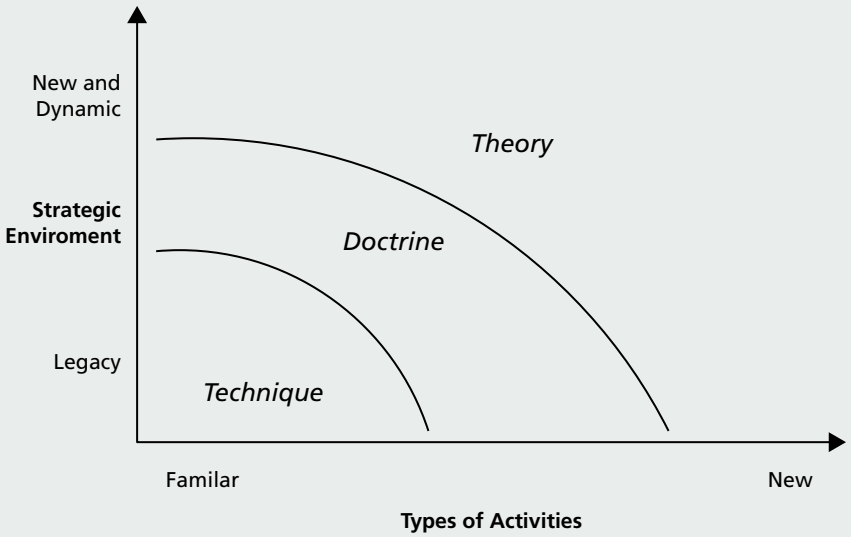
Third, a number of influential international organizations have arisen. Over time, their organizational capabilities have matured, their roles have expanded, their legitimacy has grown, and their influence over international and national activities has increased. Such entities provide alternative forums for the communication, cooperation, and conflict resolution that have increasingly changed the dynamics of international interaction.

Fourth, the ways and means of violent conflict have changed radically. The advent of nuclear weapons stands out as the most significant development. Advancements in communications, precision-guided munitions, and intelligence, surveillance, and reconnaissance have changed the character of war.[7] Arms proliferation including missiles and weapons of mass destruction have placed great power in more hands. Finally, the information age has introduced ubiquitous media reporting and cyber attack.[8]

Collectively, these four changes in the environment have dispersed power in the international order and altered the rules of the game for conflict resolution. Since the Peace of Westphalia in 1648, nation-states have served as the primary actors in the international arena. While they will remain the most important actors for some time, the paradigm for power distribution is changing. Large states with great resources and robust militaries now share a much greater portion of power with smaller states and nonstate actors, which can now create, control, and transact information, monetary value, and weaponry in significant ways and amounts. They often enjoy an advantage over larger states in access, agility, and anonymity. Furthermore, the transnational nature of many activities, ambiguity of certain actor identities, and perceived capabilities and legitimacy of nonstate actors erode the notion of inviolable territorial integrity and political sovereignty.[9]

Simultaneously, international norms of behavior have begun to change. Paradoxically, as the acceptability of using force to resolve state-versus-state conflict diminishes, the impetus for able states to intervene elsewhere for humanitarian causes increases. The transnational nature of certain threats such as drug-trafficking and international violent extremism complicates traditional methods of national defense. The interconnectedness of states and nonstate actors creates both opportunities and vulnerabilities that are not adequately addressed in existing national or international law. Nonstate actors enjoy increasing amounts of legitimacy, capability, and capacity to conduct activities previously reserved to states.[10] A greater number and variety of international actors may now influence issues they have stakes in. Finally, due to increased interconnectedness, events in one place often have more extensive second- and third-order effects on a greater variety of entities and across a larger span of the globe. The

Figure 1. Contextual View of Cyber Attack and Associated Approaches



rise of nonstate actors, the interconnectedness of activities, and the ambiguity of where cyber attack fits within existing norms contorts international rules of the game.[11]

Consequently, cyberspace—which is both a cause and product of this new and dynamic environment—continues to grow as a medium for international cooperation and conflict. Cyber attack not only offers the opportunity to do new things, but it also does so in a notably different and dynamic strategic environment that demands innovative ways of thinking. The degree to which actors share these views and behave accordingly affects how they approach cyber attack issues (see figure 1). A cyber attack intended to execute a familiar task in a legacy environment is primarily a technical problem to solve. It calls for a new technique. A cyber attack reflecting newer types of activities or occurring in a new strategic environment requires not only technical innovations, but also new principles to guide operations—that is, new doctrine. Actors who believe the emergence of the cyber domain creates fundamentally new possibilities, especially in light of a vastly different and dynamic strategic environment, operate in boundary conditions that require pioneering ways to think about the problem—or new theory.[12] The steps from technique to doctrine to theory reflect nonlinear leaps in approach.[13] The contextual view an actor takes drives its approach to the remaining three elements of the framework and, ultimately, the character of resulting policy and strategy.

Spectrum of Cyber Attacks. The second element of the framework involves the extent to and ways in which an actor distinguishes between different types of cyber attacks. For example, some place various cyber attacks into the categories of war, terrorism, crime, espionage, operational preparation of the environment, and so forth.[14] Others limit discussion of cyber attacks to conflicts involving only computer network attacks or state actors.[15] Still others categorize cyber attacks according to their technical characteristics, lumping them into groups such as worms, viruses, and denial-of-service attacks.[16] These parameters provide useful frameworks for analysis, but they entail various biases or limitations. Each arranges cyber attacks by one or more of the following factors: attacker, target, victim, activity, effect, and intent. An assessment of these six factors provides insight into how broadly and in what ways various actors perceive the spectrum of cyber attacks.[17]

The first factor addresses the identity of the *attacker*, who could be an individual, multinational corporation, organized armed group such as a terrorist or insurgent entity, transnational criminal organization, traditional state, or international governmental organization. A mix of entities could work as sponsors, proxies, or partners, and any of the above could hire cyber attack mercenaries.[18]

A virtual or physical *target*, the second factor, constitutes the direct object of the actions. Objects can include information itself; digital, electronic, and mechanical systems; physical items; and the people and processes associated with any of these. Additionally, targets could involve governmental, military, corporate, private civilian, critical infrastructure, informational, financial, and intellectual property objects.[19]

The third factor, the *victim*, is the indirect object of the attacks or the owner, operator, possessor, or beneficiary of the target. Victims can include all the same types of actors as attackers. Additionally, attackers might direct strikes at particular societies, populations, or subsets. In some cases, attackers desire to gain some benefit for themselves without concern for the victim's identity per se. An attack could have multiple victims.

The fourth factor, *activity*, addresses the action that actually constitutes a cyber attack. Actions that involve both a cyber input and output include access (for example, piracy, theft, espionage); manipulation to add, delete, or change electronic data; control of computer processes; and denial of access, manipulation, or control by the victim. Actions could also involve cyber inputs with physical outputs such as malware that physically damages electronic devices, manipulates supervisory control and data acquisition (SCADA) equipment, or controls automated, robotic, and weapons systems. Finally, actions could involve noncyber (often kinetic) input with cyber output such as severing electric power to physical components of cyberspace, physical damage to those components, and an electromagnetic pulse that erases digital data or renders computing devices nonfunctional.[20] The activity may involve many actions in sequence or simultaneously.

Activities—whether cyber-cyber, cyber-physical, or noncyber-cyber—produce effects, the fifth factor. *Effect* describes not just the immediate outcome of an attack, but also the associated intensity, frequency, scope, magnitude, duration, and criticality.[21] Notable thresholds include whether the attacker actually changed the target or merely observed and accessed it, activated malware or only emplaced it, achieved virtual or physical outcomes, or caused physical damage including human injury or death.[22] This factor also encompasses second- and third-order effects[23] as well as unintended consequences.[24] The full extent of effects may be difficult to anticipate before an attack and measure afterward. Causal linkages and degrees of separation between action and result may be ambiguous.[25] Moreover, the nature of the attack and of the target, along with the victim's response,

may alter effects and a system's resiliency to them.

Finally, *intent* is the underlying purpose of the attacker in conducting a cyber attack. The attacker may desire to drive changes to political views, actions, or outcomes. Alternatively, he may want to gain an economic benefit or deny one to the victim. The attacker may hope to deny, degrade, or destroy a military or other type of capability. Or he may just want to *hurt* the victim or cause general disruption.[26] Intent reflects the motivation.[27]

Collectively, the nature of the attacker, target, victim, activity, effect, and intent characterize where a particular cyber attack fits along the spectrum of possibilities. Different combinations of these factors may produce qualitatively different kinds of cyber attacks. Certain types of attack may be more effective in specific circumstances. They present different threats and may require different postures for deterrence and responses.[28] Either an attacker or a potential victim will necessarily focus its policy, strategy, and capabilities on an arranged subset of this spectrum. Understanding how these actors bound and sort the spectrum reveals how they perceive cyber attack, both as an option and as a threat.[29] Among other things, how an actor scopes and arranges the spectrum drives the prioritization and relationship of a specific cyber attack relative to other kinds of cyber attack. The next key element addresses the primacy and relationship between cyber attack and other types of actions.

Balance of Focus. The third element of the framework entails an actor's balance of focus on cyber attack as an enabling function, an independent capability, and a strategic attack. As an enabling function, cyber attack plays a supporting role to some other form of action or operation. That is not to say that this role is necessarily unimportant; cyber attack may be the critical enabler for successful achievement of an actor's objectives. Nonetheless, it is insufficient by itself.[30] The 2007 Israeli cyber attack against Syrian air defenses was such a case.

Cyber attacks can also take on identities and purposes of their own, whether they are conducted exclusively or in conjunction with other types of operations. For example, disruption of an adversary's command, control, and communications capabilities may facilitate other offensive operations, but it has an independent quality. As independent capabilities, cyber attacks could constitute single or small-scale events with narrow objectives, focused or widespread covert operations, overt military-like campaigns between belligerents, or persistent actions over extended periods to attrit an adversary's capability or will to resist.[31]

Cyber attacks intended to achieve an attacker's main objectives by striking directly at an adversary's centers of gravity constitute strategic attacks.[32] These could take several forms. First, an attacker could use a cyber attack to detrimentally affect key infrastructure, such as shutting down telecommunications or the electric power grid via attacks on SCADA systems. The Stuxnet attack on Iran's nuclear weapons program—notably, against a closed system not connected to the Internet—provides an example.[33] Second, an attacker could disrupt critical civilian or military functions. Third, an attacker could destroy, disrupt, or deny use of a significant portion of cyberspace itself with major second-order effects on other critical functions. For example, Russia's 2008 denial-of-service attacks against Georgia's Internet infrastructure for 19 days degraded the target country's military command and control, stopped all electronic transactions of the National Bank for 10 days, and disrupted reporting of current events outside the country.[34] Vulnerability to such strategic attacks varies widely by actor depending largely on the interconnectedness of critical infrastructure such as electric power, financial institutions, and telecommunications.

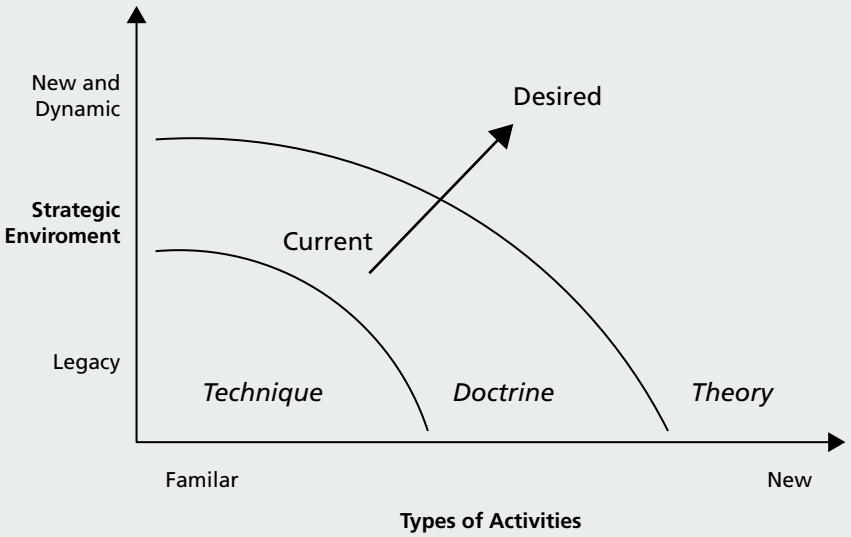
The balance of focus among these roles carries significant implications. Allocation of time, money, and expertise to develop and conduct various kinds of cyber attack reflects an actor's beliefs about desirable objectives, the direct and indirect effects possible, the most efficient use of available resources, and the efficacy of cyber attack versus other suitable instruments. The actor's contextual views and assessment of the cyber attack spectrum will largely shape these beliefs. For example, some contend that cyber attack has "broken the evolutionary continuity of the character of war"[35] and could independently achieve catastrophic strategic-level damage to critical infrastructure and disruption to societies.[36] More skeptical analysts conclude that enduring and widespread catastrophic damage remains improbable in the first place, and—even if it did occur—it would be unlikely to achieve the underlying strategic goals of the attacker.[37] Others think that strategic attacks are possible and even likely; however, their effects, while significant, may not be catastrophic.[38] An actor's views on the efficacy of enabling, independent, and strategic roles for cyber attack drive its allocation of resources, organizational alignments, development of theory and doctrine, and ultimately the associated policy and strategy. These views also shape the actor's determination of when to conduct cyber attack.

Appropriate Circumstances. The fourth element addresses the appropriate circumstances in which to conduct cyber attack. An actor must assess the opportunities and associated risks as well as the costs and benefits. As circumstances vary, so will assessments of suitability and acceptability as viewed through the lenses of law, ethics, and prudence.

Through the lens of law, two fundamental debates are under way that are interwoven and sometimes confused. The first takes a descriptive and explanatory approach to determine the legality of various cyber attacks under existing international law.[39] The second takes a normative approach to establish when and which cyber attacks *should* be lawful. Each of the six factors of the cyber attack spectrum plays a pivotal role in both debates, for delineations between legal and illegal often hinge on the particulars of one or more of those factors.[40] Additionally, difficulties with clear attribution complicate these judgments. Absent strong cyber attack precedent, it remains unclear how various actors will apply the principles and how such norms will evolve over time.[41] These issues become further convoluted when they involve nonstate actors. While certain components of international law address actions by these groups, the traditional law of armed conflict (LOAC) focuses on state-on-state engagement.[42] It seems plausible that some attackers will exploit this ambiguity to conduct cyber attacks in a manner they perceive to reside just below the thresholds of LOAC.[43]

Given the ambiguities of interpreting and applying international law, ethical norms become even more relevant. For example, even if an *armed conflict* clearly exists and a cyber attack clearly rises to the level of *use of force* or *armed attack*, actors will still make judgments in applying principles such as military necessity, proportionality, discrimination, and minimizing unnecessary human suffering in the context of cyber attacks and their associated effects.[44] Ethical norms based on religious values, ethnicities, local traditions, and other

Figure 2. Current and Desired U.S. Contextual Views of Cyber Attack



factors will vary across international actors.[45] Furthermore, regardless of how clearly or consistently actors apply LOAC, the spectrum of cyber attacks includes a huge range of activity. Much (if not most) of this activity will never rise to the level of armed conflict. While other laws including the Convention on Cybercrime, human rights law, and various national laws may apply, evolving international norms will guide how expansive or restrictive cyber attack standards become.[46] Over time, these norms will form the basis of new international rules of the game, interpretations of existing law, and creation of new law, but this process takes time.[47]

In addition to legal and ethical considerations, actors will also judge whether cyber attack in general and a specific kind in particular seems prudent. Indeed, actors may deem a cyber attack illegal and unethical and still judge it worth conducting. A number of factors may make cyber attack an appealing option. It may provide an asymmetric capability against an otherwise superior adversary. Traditional warfare is costly in treasure, lives, and political capital.[48] The low cost of entry for cyber attack allows smaller, poorer states as well as nonstate actors a seat at the table. The complexity and costs of certain high-end cyber attack operations restricts this portion of the spectrum to wealthy actors with robust capabilities; however, others can access a significant portion of the spectrum with more moderate costs and technical requirements.[49] Additionally, anonymity seems useful and achievable via cyber attack.[50] Finally, cyber attack may offer the best—and perhaps only—option for achieving certain effects.

Correspondingly, a variety of factors might dissuade an actor. Cyber attack might not offer a viable solution with the desired effect and reliability. Such activity might prove politically difficult with either internal or external audiences. Cyber attack might pose unacceptable harmful consequences to others or oneself.[51] An attacker might not want to bear the associated risk of retribution or escalation. Finally, the would-be attacker might not possess the technical capability to reliably plan or execute the desired attack. Evaluation of opportunities and risks as well as the benefits and costs would vary across actors and circumstances. However, how a particular actor perceives, weighs, and judges legal, ethical, and prudential considerations would guide its determination of the appropriate circumstances in which to conduct cyber attacks.

Implications for the United States

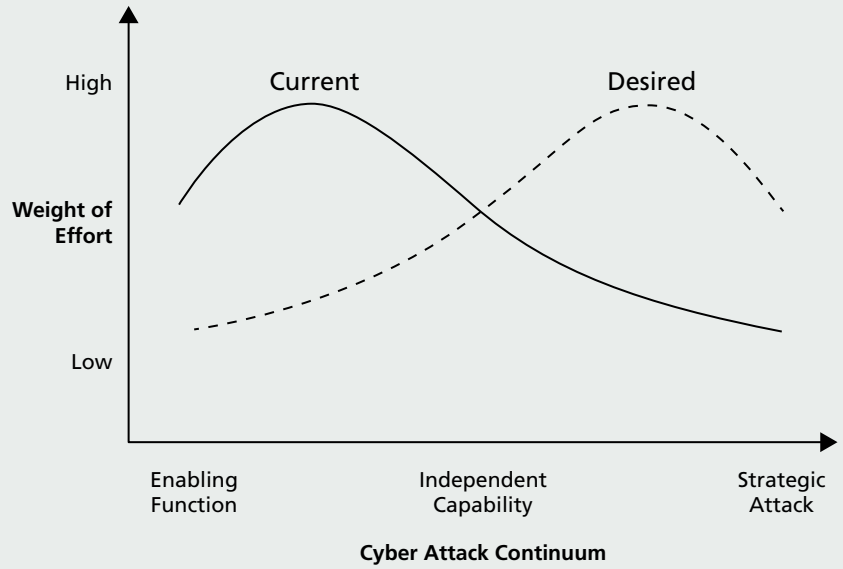
This framework provides a useful tool for U.S. policymakers and strategists. Various studies and reports have suggested the United States needs national debate and a clear cyber attack policy.[52] The elements of this framework provide the necessary foundation for conducting such discourse and formulating national guidance. How policymakers and strategists address these four core areas should drive resolution of the many more detailed operational, technical, and organizational issues that follow from them.

Context. To the extent that prevailing U.S. thinking on cyber attack has coalesced at all, it falls largely within the middle range of both the activity type and strategic environment dimensions of context. At least in public discourse, it focuses largely on cyber attacks to execute relatively familiar tasks and on certain elements of cyber security. It also tends to use the language of a legacy strategic environment dominated by state sovereignty, territorial integrity, physical interaction, and clearer distinctions between armed conflict, crime, espionage, and diplomacy. Significant pioneering effort is still needed to merge intellectual work on the new and dynamic strategic environment with the revolutionary aspects of cyber attack activities.[53] This territory offers the greatest promise of meaningful cyber attack theory that should form the basis of U.S. policy and strategy going forward (see figure 2).[54] Technology alone—especially while rapidly changing—cannot provide this foundation.[55] Theory and technology should jointly drive doctrine and the national guidance under which it is employed.[56]

Spectrum. Such theory would almost certainly steer policymakers and strategists to a wide-spectrum view of cyber attack. Distinctions between categories of cyber attacks such as war, terrorism, crime, and espionage—and the actors who conduct them—continue to blur.[57] Moreover, the actions required to conduct or respond to cyber attack would increasingly involve more coordinated participation by military, civilian government, private sector, and international entities.[58] Consequently, U.S. policy and strategy should address a broad range of cyber attacks including cyber-to-cyber, noncyber-to-cyber, and cyber-to-physical. The last category will gain increasing importance as "critical mass" is achieved in automation, robotics, and machine learning.[59] Still, some threshold is necessary to focus limited resources. For this purpose, effect—including indirect and cumulative aspects—should play an important role.

Balance. Similarly, the United States should consciously determine the balance of its efforts along the enabling, independent, and strategic attack continuum. The weight of effort currently favors enabling functions. This disposition reflects the underdeveloped nature of cyber attack theory and proclivity to operate within established realms of activity. However, the United States would benefit more from a distribution of effort weighted

Figure 3. Current and Desired U.S. Balance of Focus



toward the strategic attack end of the continuum (see figure 3). First, such an orientation induces deeper thinking for newer types of activities where the United States stands to gain the most and enemies could pose the greatest threat. Second, intentional focus on the strategic end has cascading benefits on the enabling end, where legacy organizational inertia will continue to make advances regardless; however, the reverse is much less likely. Third, cyber attack can play a niche role as a form of coercive diplomacy somewhere short of armed attack. It may also prove itself as an asymmetric advantage against nonstate actors who are less vulnerable to kinetic strikes but become more dependent on cyberspace. Both roles are more likely found on the independent and strategic attack end. Fourth, given the dynamic nature of cyber attack technology, the United States should adopt a future-oriented perspective. It is better to be constrained by technology than ideas. Finally, policymakers and strategists should devote concerted effort on the linkage between the direct effects of cyber attack and the desired political, security, and economic outcomes—a key element of more mature theory.[60]

Circumstances. Determining the appropriate circumstances in which to conduct cyber attack may prove elusive, but it could also produce the most direct consequences. U.S. policy should preserve the stability of international laws and norms regarding armed conflict. However, because both the strategic environment and the activities afforded by technology—both bases for existing laws and norms—have changed in fundamental ways, some recalibration is required. As previously argued, the rules of the game are changing. How large a role will the United States play in what they change to?

Superpower status, allure as a target, and cyber attack capability make the United States uniquely positioned to lead that recalibration. Positions taken (or not taken) and actions conducted (or not conducted) could set precedents and sow norms with far-reaching consequences.[61] Assuming a strong alignment between what is beneficial for the United States and for the rest of the world in terms of international security and stability, Washington should take a normative approach. That is, policymakers should first determine what international norms *ought* to exist vis-à-vis cyber attack. Then they should emplace policies to build international consensus, set precedent, interpret relevant existing international law, develop norms of behavior, and draft new agreements (treaty law) as appropriate to institutionalize those normative determinations. In this way, the United States can lead the modernization of international law in a way that accounts for the fundamental contextual changes of cyber attack.[62]

Washington should maintain stability and order by limiting cyber attacks while also preserving options to conduct such attacks in defense of its interests. This duality exists for other forms of statecraft, especially armed conflict, but it does beg the question of when it makes sense to conduct, or at least threaten, cyber attack. Assuming that a particular cyber attack is possible, U.S. policymakers and strategists should evaluate its suitability and acceptability. Suitability addresses causal linkages between a given cyber attack and desired outcomes. In other words, using the logic of cyber attack, one should explain how the particular attack results not only in the direct effects but also in the desired modification to environmental conditions or adversarial behavior.[63] To inform such evaluations, especially in the absence of sufficient empirical case studies, one needs sound theory that addresses how to impose, defend, coerce, deny, compel, and deter vis-à-vis cyber attack.[64]

If cyber attack offers a suitable option, one should assess its acceptability. Acceptability addresses the conditions created by a cyber attack. Will others perceive the attack as violent? Does it intentionally (or likely) result in human injury or death, other human suffering, physical damage or destruction, or loss of critical data? What collateral damage may result? Are these effects irreversible? What is the current state of affairs and status of conflict, does traditional armed conflict already exist, and to what extent does the cyber attack risk escalation? Does the attack involve highly sensitive areas, such as the international finance system or weapons of mass destruction, which could undermine trust, confidence, and reliability; set far-reaching negative precedent; create uncontrollable systemic repercussions; or produce otherwise taboo effects?[65] Most fundamentally, does the attack contribute to or detract from long-term international security and stability as well as the norms that promote them? Given answers to these and similar questions, is the cyber attack acceptable to the United States? To the international community?

These questions address normative legal, ethical, and prudential aspects of cyber attack that should guide U.S. policy and strategy, but answering them is difficult. Well-developed cyber policy and strategy, as with nuclear issues in the last century, will evolve over time; however, it should begin with a clear idea of *what* the United States is trying to achieve and *how* that might come to pass. Those ideas should be grounded in well-developed cyber attack theory, distinct understanding of the cyber attack spectrum, and appropriately weighted effort along the cyber attack continuum.

Vice Admiral Michael Rogers, USN, commander U.S. Fleet Cyber Command and U.S. 10th Fleet, speaks to Information Dominance Corps Sailors at U.S. Naval Forces Southern Command

U.S. Navy (Robert Wood, Sr.)

National governments do not yet have well-defined cyber attack policies and strategies, a condition exacerbated by accelerating changes in power distribution, cyber technology, and other dynamics of the strategic environment. Contextual views of cyber attack, the cyber attack spectrum, balance of focus, and appropriate circumstances constitute a foundational framework upon which international actors could build such strategic guidance. For the United States in particular, the proposed approaches to each element lay a foundation for coherently shaping national guidance and international norms. A progressive view of both new types of activities and the dynamic new strategic environment in which they occur should form the impetus for developing more comprehensive cyber attack theory. Additionally, a wide-spectrum view that takes a more nuanced approach to categorizing cyber attacks combined with a focus toward the strategic attack end of the cyber attack continuum will properly shape U.S. perspective. Consequently, such perspective will inform a normative approach for determining the appropriate circumstances in which to conduct cyber attack, which will guide both U.S. action and modernization of international norms. The journey to open, distinct, and explicit cyber attack policy and strategy will take time. However, this framework starts the United States down a deliberate path toward a more desirable—if yet to be determined—destination. **JFQ**

NOTES

[1] William A. Owens, Kenneth W. Dam, and Herbert S. Lin, eds., *Technology, Policy, Law, and Ethics Regarding U.S. Acquisition and Use of Cyberattack Capabilities* (Washington, DC: National Academies Press, 2009), 59.

[2] I am indebted to General Michael P.C. Carns, USAF (Ret.), Martin C. Libicki, and Joseph S. Nye, Jr., for their suggestions on framing this research.

[3] Williamson Murry, MacGregor Knox, and Alvin Bernstein, eds., *The Making of Strategy: Rulers, States, and War* (New York: Cambridge University Press, 1994), 3–6, 22.

[4] Richard A. Clarke and Robert K. Knake, *Cyber War: The Next Threat to National Security and What to Do About It* (New York: HarperCollins, 2010), 5–8.

[5] The land, maritime, air, and space domains all exist naturally and, in general, possess physical delineations from each other. Even before the technology emerged to leverage the latter three for warfighting and other human purposes, the domains themselves existed. Cyberspace is fundamentally different. It is entirely created by man and is both physical and virtual, as well as mutable. It consists of the world's computers and the open and closed networks that connect them (including but not limited to the Internet and telecommunications networks): the hardware, network infrastructure, software, resident data and information, and arguably the human operators of these elements. See Franklin D. Kramer, Stuart H. Starr, and Larry K. Wentz, *Toward a (Preliminary) Theory of Cyberpower* (Washington, DC: Center for Technology and National Security Policy, June 2008), 22–26, available at <www.dtic.mil/dtic/tr/fulltext/u2/a486839.pdf>; Joseph S. Nye, Jr., *The Future of Power* (New York: PublicAffairs, 2011), 122.

[6] Greg Rattray, Chris Evans, and Jason Healey, "American Security in the Cyber Commons," in *Contested Commons: The Future of American Power in a Multipolar World*, ed. Abraham M. Denmark and James Mulvenon, 143 (Washington, DC: Center for a New American Security, January 2010).

[7] Eliot A. Cohen, "The Mystique of U.S. Air Power," *Foreign Affairs*, January–February 1994, 109–124.

[8] Interestingly, civil resistance researchers report that both the frequency and success rate of nonviolent resistance by nonstate actors against incumbent regimes and occupiers increased from 1900 to 2006. While not a focus of their work, cyber attack could play an important role in such resistance as a nonviolent (that is, does not cause physical harm) action—legal or illegal—or as a means of suppression by the target regime. See Erica Chenoweth and Maria J. Stephan, *Why Civil Resistance Works: The Strategic Logic of Nonviolent Conflict* (New York: Columbia University Press, 2011), 6–15.

[9] Nye, *The Future of Power*, 113–122: "Two great power shifts are occurring in this century: a power transition among states and a power diffusion away from all states to nonstate actors" (xv).

[10] Michael N. Schmitt, "Cyber Operations in International Law: The Use of Force, Collective Security, Self-Defense, and Armed Conflicts," in *Proceedings of a Workshop on Deterring Cyber-Attacks: Informing Strategies and Developing Options for U.S. Policy* (Washington, DC: The National Academies Press, 2010), 173–176, available at <www.nap.edu/catalog/12997.html>.

[11] Arthur K. Cebrowski, "Foreword," in *Rethinking the Principles of War*, ed. Anthony McIvor, xii (Annapolis: Naval Institute Press, 2005).

[12] Milan Vego, "On Military Theory," *Joint Force Quarterly* 62 (3rd Quarter 2011), 60, available at <www.ndu.edu/press/lib/images/jfq-62/JFQ62_59-67_Vego.pdf>.

[13] James M. Dubik, "Introduction: Get on with It," in *Rethinking the Principles of War*, ed. Anthony McIvor, 1–2 (Annapolis: Naval Institute Press, 2005).

[14] Nye, *The Future of Power*, 144; Clarke and Knake, *Cyber War*, 197–200.

[15] Martin C. Libicki, *Cyberdeterrence and Cyberwar* (Santa Monica, CA: RAND, 2009), 117, available at <www.rand.org/multimedia/video/2012/02/22/cyberdeterrence-cyberwar.html>.

[16] Gregory Rattray and Jason Healey, "Categorizing and Understanding Offensive Cyber Capabilities and Their Use," in *Proceedings of a Workshop on Deterring CyberAttacks*.

[17] Ibid., 81–83. Rattray and Healy use 12 factors to categorize offensive cyber operations. They focus on offensive operations analogous to computer network attack (excluding cyber espionage) conducted "between political actors operating across state boundaries or by nonstate actors for political purposes" (77).

[18] Ibid., 82.

[19] Ibid.

[20] Greg Rattray, *Strategic Warfare in Cyberspace* (Cambridge, MA: MIT Press, 2001), 18. Rattray's dissertation on which this book is based, "Strategic Information Warfare: Challenges of the United States" (The Fletcher School of Law and Diplomacy, May 1998), is available at <www.dtic.mil/cgi-bin/GetTRDoc?Location=U2&doc=GetTRDoc.pdf&AD=ADA346502>.

[21] Rattray and Healey, 82.

[22] Clarke and Knake, 197–200.

[23] John Rollins and Clay Wilson, *Terrorist Capabilities for Cyberattack: Overview and Policy Issues*, RL33123 (Washington, DC: Congressional Research Service, January 22, 2007), 3, available at <www.fas.org/sgp/crs/terror/RL33123.pdf>.

[24] Unintended consequences, or spillover effects, may have positive or negative value from the perspective of the attackers. *Collateral damage* is a related, but not entirely equivalent concept.

[25] Schmitt, "Cyber Operations in International Law," 156–157.

[26] Thomas C. Schelling, *Arms and Influence* (New Haven: Yale University Press, 2008), 2.

[27] Libicki, *Cyberdeterrence and Cyberwar*, 75–90.

[28] Rattray and Healey, 82.

[29] Rollins and Wilson, 19–25.

[30] Libicki, *Cyberdeterrence and Cyberwar*, 140–141.

[31] Ibid., 86–91.

[32] Rattray, 14.

[33] Andrew F. Krepinevich, *Cyber Warfare: A "Nuclear Option"?* (Washington, DC: Center for Strategic and Budgetary Assessments, 2012), 62–65, available at <www.csbaonline.org/wp-content/uploads/2012/08/CSBA_Cyber_Warfare_For_Web_1.pdf>.

[34] 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 (3rd Quarter 2012), 22.

[35] Giulio Douhet, *The Command of the Air*, trans. Dino Ferrari (1942; rpt. Washington, DC: U.S. Government Printing Office, 1998), 180, available at <www.afhso.af.mil/shared/media/document/AFD-100924-017.pdf>.

[36] Clarke and Knake, 30–31.

[37] Libicki, "Chapter 6: Strategic Cyberwar," in *Cyberdeterrence and Cyberwar*, 117–137.

[38] Rattray, 120.

[39] The North Atlantic Treaty Organization's Cooperative Cyber Defence Centre of Excellence has produced the draft *Tallinn Manual*, a collective effort of experts to determine how the existing law of armed conflict applies to cyber attacks; however, this document reflects personal or collective views but not necessarily the views of states. It is neither binding nor sets precedent. Available at <www.ccdcoe.org/249.html>. See also Harold Hongju Koh, "International Law in Cyberspace: Remarks of Harold Koh," *Harvard International Law Journal Online* 54 (December 2012), available at <www.harvardilj.org/2012/12/online_54_koh/>; and Michael N. Schmitt, "International Law in Cyberspace: The Koh Speech and Tallinn Manual Juxtaposed," *Harvard International Law Journal Online* 54 (December 2012), available at <www.harvardilj.org/2012/12/online-articles-online_54_schmitt>.

[40] For example, in the context of *jus ad bellum*, debate centers on whether a cyber attack equates to a *use of force* or an *armed attack*. Some argue that the determination hinges on the consequences of the cyber attack rather than the instrument of attack itself. However, language in the United Nations Charter involves the manner of attack, as it was written prior to the emergence of cyber attacks when military force between state actors presented the primary threat. Some argue that if cyber attack effects resemble those of other military force generally considered *armed attack*, the cyber attack will likely be considered an armed attack. Similarly, if cyber attack effects resemble those of harmful actions (political, economic, or covert) that do not otherwise rise to the level of *use of force*, the cyber attack will not likely be considered such. See Owens, Dam, and Lin, 251–252, 272.

[41] Ibid., 262–272.

[42] Ibid., 273–277.

[43] Rattray and Healey, 89–90.

[44] Martin C. Libicki, *Crisis and Escalation in Cyberspace* (Santa Monica, CA: RAND, 2012), 29–35, available at <www.rand.org/content/dam/rand/pubs/monographs/2012/RAND_MG1215.pdf>.

[45] Owens, Dam, and Lin, 240.

[46] Ibid., 277–282.

[47] Schmitt, "Cyber Operations in International Law," 177.

[48] Daniel Wagner and John Margeson, "The Globalization of Covert Action," *Huffington Post Online*, September 9, 2012, available at <www.huffingtonpost.com/daniel-wagner/globalization-of-covert-action_b_1869134.html>.

[49] Nye, *The Future of Power*, 117, 124–125; Rattray, 464.

[50] Martin C. Libicki, "The Specter of Non-obvious Warfare," *Strategic Studies Quarterly* 6, no. 3 (Fall 2012), 91–92, available at <www.au.af.mil/au/ssq/2012/fall/fall12.pdf>.

[51] Owens, Dam, and Lin, 241.

[52] For example, see ibid., 57–62; Clarke and Knake, 261–264.

[53] Joseph S. Nye, Jr., "Nuclear Lessons for Cyber?" *Strategic Studies Quarterly* 5, no. 4 (Winter 2011), 18, 23, 36, available at <www.au.af.mil/au/ssq/2011/winter/winter11.pdf>.

[54] Vego, 60; Clarke and Knake, 151–155.

[55] Nye, "Nuclear Lessons for Cyber?" 24–25.

[56] Herman Kahn, *On Thermonuclear War* (New Brunswick, NJ: Transaction, 2007), 3–4, 38–39, 532, 576.

[57] Nye, *The Future of Power*, 144–145.

[58] Nye, "Nuclear Lessons for Cyber?" 26–29, 36.

[59] Bill Gates, "A Robot in Every Home," *Scientific American Online*, December 16, 2006, available at <www.scientificamerican.com/article.cfm?id=a-robot-in-every-home>; Peter W. Singer, *Wired for War* (New York: Penguin Press, 2009), 7–11.

[60] Rattray, 120.

[61] Schelling, 153–168, discusses the conditions conducive for *precedent* to become *norm*.

[62] Schmitt, "Cyber Operations in International Law," 177–178.

[63] A complete evaluation includes an appreciation of probability of outcome and level of confidence in the estimate.

[64] Schelling, 4–5, 69–78; Nye, "Nuclear Lessons for Cyber?" 25–26. Cyber attack could be the method (for example, a cyber attack to compel adversary action) or the object (for example, to deter cyber attack by the adversary). Also, cyber attack could be conducted alone or in conjunction with other instruments such as economic sanctions and kinetic strikes.

[65] Clarke and Knake, 197–209.