Strategy Research Project

Four Core Questions for U.S. Cyberattack Guidance

by

Colonel Jonathan C. Rice IV
United States Air Force

United States Army War College
Class of 2013

DISTRIBUTION STATEMENT: A
Approved for Public Release
Distribution is Unlimited

This manuscript is submitted in partial fulfillment of the requirements of the Master of Strategic Studies Degree. The views expressed in this student academic research paper are those of the author and do not reflect the official policy or position of the Department of the Army, Department of Defense, or the U.S. Government.

The U.S. Army War College is accredited by the Commission on Higher Education of the Middle States Association of Colleges and Schools, 3624 Market Street, Philadelphia, PA 19104, (215) 662-5606. The Commission on Higher Education is an institutional accrediting agency recognized by the U.S. Secretary of Education and the Council for Higher Education Accreditation.

REPORT DOCUMENTATION PAGE	*Form Approved* *OMB No. 0704-0188*

1. REPORT DATE *(DD-MM-YYYY)*
xx-03-2013

2. REPORT TYPE
STRATEGY RESEARCH PROJECT

3. DATES COVERED *(From - To)*

4. TITLE AND SUBTITLE
Four Core Questions for U.S. Cyberattack Guidance

5a. CONTRACT NUMBER

5b. GRANT NUMBER

5c. PROGRAM ELEMENT NUMBER

6. AUTHOR(S)
Colonel Jonathan C. Rice IV
United States Air Force

5d. PROJECT NUMBER

5e. TASK NUMBER

5f. WORK UNIT NUMBER

7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES)
Dr. Stephen J. Gerras
Department of Command, Leadership, and Management

8. PERFORMING ORGANIZATION REPORT NUMBER

9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)
U.S. Army War College
122 Forbes Avenue
Carlisle, PA 17013

10. SPONSOR/MONITOR'S ACRONYM(S)

11. SPONSOR/MONITOR'S REPORT NUMBER(S)

12. DISTRIBUTION / AVAILABILITY STATEMENT
Distribution A: Approved for Public Release. Distribution is Unlimited.

13. SUPPLEMENTARY NOTES
Word Count: 5743

14. ABSTRACT
National governments, including that of the United States, do not yet have well-formed cyberattack policies and strategies. A proposed framework consisting of four foundational elements—contextual views, the cyberattack spectrum, balance of focus, and appropriate circumstances—provides a basis for considering, discussing, developing, and assessing strategic cyberattack guidance. How an actor approaches each of these four elements fundamentally shapes the myriad details of subsequent policy and strategy. In view of this framework, the United States should pursue development of comprehensive cyberattack theory. Additionally, it should adopt a broader, but more nuanced view of cyberattacks combined with a focus weighted toward strategic attack. Consequently, such perspective will inform a normative approach for determining the appropriate circumstances in which to conduct cyberattack, which will guide both U.S. action and modernization of international norms.

15. SUBJECT TERMS
Cyberspace, Cyberpower, Cyberwar, Strategic Environment, Law of Armed Conflict, National Security Strategy

16. SECURITY CLASSIFICATION OF:			**17. LIMITATION OF ABSTRACT**	**18. NUMBER OF PAGES**	**19a. NAME OF RESPONSIBLE PERSON**
a. REPORT UU	**b. ABSTRACT** UU	**c. THIS PAGE** UU	UU	36	**19b. TELEPHONE NUMBER** *(Include area code)*

USAWC STRATEGY RESEARCH PROJECT

Four Core Questions for U.S. Cyberattack Guidance

by

Colonel Jonathan C. Rice IV
United States Air Force

Dr. Stephen J. Gerras
Department of Command, Leadership, and Management
Project Adviser

This manuscript is submitted in partial fulfillment of the requirements of the Master of Strategic Studies Degree. The U.S. Army War College is accredited by the Commission on Higher Education of the Middle States Association of Colleges and Schools, 3624 Market Street, Philadelphia, PA 19104, (215) 662-5606. The Commission on Higher Education is an institutional accrediting agency recognized by the U.S. Secretary of Education and the Council for Higher Education Accreditation.

The views expressed in this student academic research paper are those of the author and do not reflect the official policy or position of the Department of the Army, Department of Defense, or the U.S. Government.

U.S. Army War College
CARLISLE BARRACKS, PENNSYLVANIA 17013

Abstract

Title:	Four Core Questions for U.S. Cyberattack Guidance
Report Date:	March 2013
Page Count:	36
Word Count:	5743
Key Terms:	Cyberspace, Cyberpower, Cyberwar, Strategic Environment, Law of Armed Conflict, National Security Strategy
Classification:	Unclassified

National governments, including that of the United States, do not yet have well-formed cyberattack policies and strategies. A proposed framework consisting of four foundational elements—contextual views, the cyberattack spectrum, balance of focus, and appropriate circumstances—provides a basis for considering, discussing, developing, and assessing strategic cyberattack guidance. How an actor approaches each of these four elements fundamentally shapes the myriad details of subsequent policy and strategy. In view of this framework, the United States should pursue development of comprehensive cyberattack theory. Additionally, it should adopt a broader, but more nuanced view of cyberattacks combined with a focus weighted toward strategic attack. Consequently, such perspective will inform a normative approach for determining the appropriate circumstances in which to conduct cyberattack, which will guide both U.S. action and modernization of international norms.

Four Core Questions for U.S. Cyberattack Guidance

> One of the most obvious lessons of history is that the preservation of
> States and civilization lies in the ability to allow for changed conditions.
>
> —P.R.C. Groves[1]

In 1903, the Wright Brothers ushered in the age of airpower, granting mankind access to the air as an arena in which it could meaningfully conduct activities as individuals, as institutions, or as states. In 1957, the Soviet Union launched Sputnik I, the world's first artificial satellite, thereby jumpstarting the space age. With somewhat less fanfare in 1969, a University of California, Los Angeles computer user transmitted the first Advanced Research Projects Agency Network (ARPANET) message to a Stanford Research Institute system. By the time the term *cyberspace* was coined 15 years later, ARPANET had become the Internet, Transmission Control Protocol/Internet Protocol (TCP/IP) had become the standard networking protocol, microprocessors had been developed, personal computers had come to market, and the first graphical user interface had been introduced. Humanity had not just gained access to cyberspace; it had *created* this new realm of existence and activity. During this same period, the first computer worms and viruses appeared; thus, *cyberattack* was born.[2]

The last decade has seen a lot of writing about cyberpower, cyberwar, and cyberattack. Nonetheless, many unresolved questions about the potential and implications of these concepts remain. In particular, national governments, including that of the United States, do not yet have well-formed cyberattack policies and strategies, or the frameworks around which to build such things.[3] Further, the accelerating changes in power distribution, cyber technology, and other dynamics of the strategic environment exacerbate the dearth of open, distinct, and explicit cyberattack policies and strategies.

If such well-defined guidance existed (or to the extent that it does), what questions would one reasonably expect it to answer? Upon what intellectual foundation should a state build its cyberattack policy and strategy? From another perspective, if an outsider wanted to understand an actor's policy and strategy, for what clues would it look? Answers to these questions could—and this paper argues *should*—reside in four foundational elements: contextual views, the cyberattack spectrum, balance of focus, and appropriate circumstances. How an actor approaches each of these four elements fundamentally shapes the myriad details of subsequent policy and strategy. This paper will first present a framework based on these elements for considering, discussing, developing, and assessing cyberattack policies and strategies of state and non-state actors. It will then use that framework to highlight implications and make recommendations for U.S. national guidance.[4]

Framework for Cyberattack Policy and Strategy

The proposed framework consists of four foundational elements for cyberattack policy and strategy. One could use this framework as a model to think about and discuss cyberattack in a structured way, as a basis for forming one's own policy and strategy, or as a tool for assessing and understanding the strategic guidance of another actor. Here are the four key elements of the framework:

1. Context: To what extent does cyberattack provide a new way to do things along two dimensions—type of activities and view of the strategic environment,

2. Spectrum: How broadly and in what arrangement does one consider the spectrum of cyberattack possibilities,
3. Focus: What is the optimal balance of focus along the continuum of cyberattack as an enabling function, an independent capability, and a strategic attack, and
4. Circumstances: What are the appropriate circumstances—legal, ethical, and prudential—in which to conduct cyberattacks?

The clarity with which an actor addresses these four key 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.[5]

Contextual View of Cyberattack – New Way, New Activities, New Environment

The first and most significant element addresses an actor's contextual view of cyberattack in terms of newness of the types of activities conducted and the strategic environment in which those activities occur. In its simplest expression, a cyberattack is just a new way to conduct an attack; cyber provides a new set of tools to accomplish familiar tasks. This is not insignificant. Israel's reported cyberattack against air defenses during a 2006 strike on a Syrian nuclear weapons facility represents such a manifestation. During the strike, Syrian radar screens did not show the incoming Israeli fighter aircraft because an Israeli cyberattack had allegedly taken control of the systems, enabling the fighters to arrive undetected.[6] Other methods have been used to negate air defenses: terrain-masking flight routes, stealth aircraft, radar jamming, kinetic strikes against air defense equipment, and severing of air defense communications lines. In this case, cyberattack allowed use of non-stealthy aircraft while concealing not just the specific location of the aircraft but also the imminence of an attack at all. Cyberattack provided some clear advantages over other available tools, but nonetheless performed a familiar task.

New Activities

However, cyberattack also offers revolutionary capabilities. 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 or other human purposes, the domains themselves existed. Cyberspace is fundamentally different. It is entirely created by man, it is both physical and virtual, and it is very mutable. Cyberspace 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 those things.[7] 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. The emergence of the cyber domain means that cyberattacks can be more than merely new tools to conduct familiar tasks. Within this realm, actors can conduct activities or achieve effects not otherwise attainable.[8] The 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 achievable through other means.

New Strategic Environment

The second dimension of the contextual view consists of the novelty and dynamic nature of the strategic environment. Four important 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, the establishment of states covering the globe, the development of international law, and the creation of institutions to help resolve disputes have significantly reduced the amount of such territory. Nonetheless, there remain a number of hotly contested border areas between states (e.g., Kashmir), nations without a state (e.g., Kurds), disgruntled people within a state (e.g., Tibetans), and un- or undergoverned areas (e.g., Somalia). Poor governance, significant economic inequities, and lack of security in such areas greatly increase the potential for conflict. In this century, these represent the territorial conditions most likely to produce conflict and the non-state actors often involved.

Second, globalization has accelerated at an exponential pace over the last few decades. The end of Cold War restraints and technological development such as improved air travel, satellite capabilities, telecommunications, computer processing, and the Internet have significantly accelerated global interconnectedness. In particular, recent decades experienced significantly increased mobility 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, particularly since the Second World War. These include the United Nations, the North Atlantic Treaty Organization, the European Union, the African Union, the World Trade

Organization, the World Bank, the Association of Southeast Asian Nations, and the Organization of American States. Over time, their organizational capabilities matured, their roles expanded, their legitimacy grew, and their influence over international and national activities increased. Such entities provide alternative fora for communication, cooperation, and conflict resolution, which have increasingly changed the dynamics of international interaction.

Fourth, the ways and means of violent conflict have changed radically. The advent of nuclear weapons clearly stands out as the most significant development. Tanks and helicopters changed land warfare. Air and space capabilities opened the third and fourth domains to warfighting. Advancements in communications, precision-guided munitions, and intelligence, surveillance, and reconnaissance changed the character of war, especially since the First Gulf War.[9] Arms proliferation, including missiles and weapons of mass destruction, placed great power in more hands. Finally, the Information Age introduced ubiquitous media reporting and cyberattack.[10]

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 non-state actors, such as international organizations, non-governmental organizations, multinational corporations, transnational criminal organizations, terrorist networks, and even some private individuals. Smaller states and non-state actors 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—where beneficial—anonymity. Further, the transnational nature of many activities, the ambiguity of certain actor identities, and the perceived capabilities and legitimacy of non-state actors erodes the notion of inviolable territorial integrity and political sovereignty.[11]

Simultaneously, the 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 non-state actors creates both opportunities and vulnerabilities not adequately addressed in existing national or international law. Non-state actors enjoy increasing amounts of legitimacy, capability, and capacity to conduct activities previously reserved to states.[12] A greater number and variety of international actors may now have a stake in and ability to influence certain issues. 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 rise of non-state actors, interconnectedness of activities, and ill fit of cyberattack within existing norms contorts existing international rules of the game.[13]

Technical, Doctrinal, and Theoretical Approaches

Consequently, cyberspace—both a cause and product of this new and dynamic environment—continues to grow as a medium for international cooperation and conflict. Cyberattack not only offers the opportunity to do new things, but 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 cyberattack issues (see Figure 1). A cyberattack intended to execute a familiar task in a legacy environment is primarily a technical problem to solve…new technique. Cyberattacks reflecting newer types of activities or occurring in a new strategic environment require not just technical innovations, but also new principles to guide operations…new doctrine. Actors who believe emergence of the cyber domain creates fundamentally new possibilities, and especially so in light of a vastly different and dynamic strategic environment, operate in boundary conditions that require pioneering ways to think about the problem…new theory.[14] The steps from technique to doctrine to theory reflect non-linear leaps in approach.[15] The contextual view taken by an actor, whether for conceptual or pragmatic reasons, drives its approach to the remaining three elements of the framework and, ultimately, the character of resulting policy and strategy.

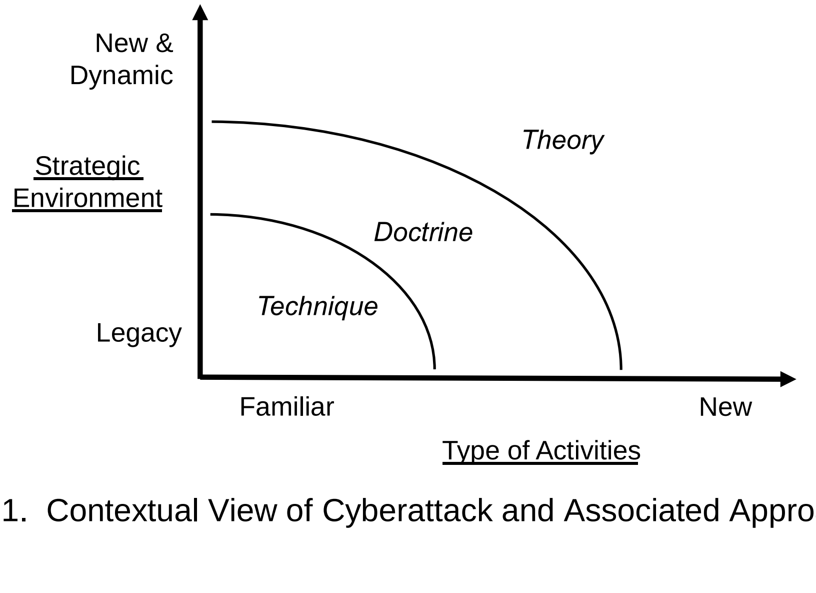

Figure 1. Contextual View of Cyberattack and Associated Approaches

Spectrum of Cyberattacks

The second element of the framework involves the extent to and ways in which an actor distinguishes between different types of cyberattacks. For example, some place various cyberattacks into the categories of war, terrorism, crime, espionage, operational preparation of the environment, and so forth.[16] Others limit discussion of cyberattacks to events involving only computer network attacks by each belligerent on the other. Some solely consider events involving at least one state actor or, in more restrictive cases, involving *only* state actors.[17] Additionally, some categorize cyberattacks according to their technical characteristics, lumping them into groups like worms, viruses, Trojan horses, and denial-of-service attacks.[18] These parameters provide useful frameworks for analysis, but they each entail various biases or limitations. Each of those categorizations arranges cyberattacks 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 cyberattacks.[19]

The first factor addresses the identity of the attacker. The attacker could consist of an individual or collection of individuals, whether acting with loose ad hoc coordination or as part of a more formal group; a multinational corporation; an organized armed group such as a terrorist or insurgent entity; a transnational criminal organization; a traditional state; or an international governmental organization. A mix of entities could work as sponsors, proxies, or partners, and any of the above could hire cyberattack mercenaries with the requisite technical capabilities.[20]

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 them. Additionally, targets could involve governmental, military, corporate, private civilian, belligerent, critical infrastructure, informational, financial, and intellectual property objects.[21]

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 attacks at particular societies, populations, or subsets of them. In some cases, attackers desire to gain some benefit for themselves without concern for the victim's identity per se. A single attack or series of attacks could have multiple victims.

The fourth factor, activity, addresses the action that actually constitutes a cyberattack. Actions that involve both a cyber input and cyber output include access (e.g., 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 or destroys 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 electro-magnetic pulse that erases digital data or renders computing devices non-functional.[22] The activity may involve many actions in sequence or simultaneously to achieve the desired effect.

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.[23] Notable thresholds often discussed in terms of cyberattack include whether the attacker actually changed the target or merely observed/accessed it, whether an attacker activated malware or just emplaced it, whether manifestation of the attack involved virtual or physical outcomes, and whether physical damage, human injury or human death resulted.[24] This factor also encompasses second- and third-order effects[25] as well as unintended consequences.[26] The full extent of effects may be difficult to anticipate before an attack and measure after an attack. Causal linkages and degrees of separation between action and result may be ambiguous.[27] Further, the nature of the attack, of the target, and of 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 cyberattack. The attacker may desire to drive changes to political views, actions, or outcomes. Alternatively, the attacker may want to gain an economic benefit or deny such to the victim. The attacker may hope to deny, degrade, or destroy a military or other type of capability. Or the attacker may just want to *hurt* the victim or cause general disruption or destruction.[28] Intent reflects the attacker's motivation to conduct a cyberattack.[29]

Collectively, the nature of the attacker, target, victim, activity, effect, and intent characterize where a particular cyberattack fits along the broad spectrum of possibilities. Different combinations of those factors may produce qualitatively different kinds of cyberattacks. Certain kinds of cyberattacks may be more suitable and effective in specific circumstances. They present different kinds of threats and may require different kinds of postures for deterrence and responses for defense.[30] An attacker—and a potential victim—will necessarily focus its policy, strategy, and capabilities on an arranged subset of this spectrum. Understanding how these actors explicitly or implicitly bound and sort the spectrum reveals how they perceive cyberattack…both as an option and as a threat.[31] Among other things, how an actor scopes and arranges the spectrum drives the prioritization and relationship of a specific cyberattack relative to other kinds of cyberattack. The next key element addresses the primacy and relationship between cyberattack and other types of actions.

Balance of Focus

The third element of the framework entails an actor's balance of focus on cyberattack as an enabling function, an independent capability, and a strategic attack. In the first, cyberattack plays a supporting role to some other form of action or operation. That is not to say that this role is necessarily unimportant; cyberattack may be the critical enabler for successful achievement of an actor's objectives. Nonetheless, it is insufficient by itself.[32] The Israeli cyberattack against Syrian air defenses in 2007 provides such a case.

Cyberattacks can also take on an identity and purpose of their own, whether 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, cyberattacks could constitute single or small-scale events with very 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.[33]

Cyberattacks intended to achieve an attacker's main objectives by striking directly at an adversary's centers of gravity constitute strategic attacks.[34] These could take several forms. First, an attacker could use a cyberattack 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.[35] 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 ten days, and disrupted reporting of current events outside the country.[36] Of course, vulnerability to such strategic attacks varies widely by actor depending largely on the interconnectedness of critical infrastructure such as electric power, water filtration, financial institutions, and telecommunications.

The balance of focus among these various roles carries significant implications. Allocation of time, money, and expertise to develop and conduct various kinds of cyberattack 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 cyberattack versus other suitable instruments. The actor's contextual views and assessment of the cyberattack spectrum will largely shape these beliefs. For example, some contend that cyberattack has "broken the evolutionary continuity of the character of war"[37] and could independently achieve catastrophic strategic-level damage to critical infrastructure and disruption to societies.[38] More skeptical analysts conclude that enduring, wide-spread catastrophic damage remains improbable in the first place, and—even if it did occur—unlikely to achieve the underlying strategic goals of the attacker.[39] Others think that strategic attacks are possible, even likely; however, their effects may be significant, but not catastrophic.[40] An actor's views on the efficacy of enabling, independent, and strategic roles for cyberattack 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 cyberattack.

Appropriate Circumstances

The fourth element addresses the appropriate circumstances in which to conduct cyberattack. 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 underway, interwoven, and sometimes confused. The first debate takes a descriptive and explanatory approach to determine the legality of various cyberattacks under existing international law. The second debate takes a normative approach to establish when and which cyberattacks ought to be lawful. Each of the six factors of the cyberattack spectrum plays a pivotal role in both of these debates, for delineations between legal and illegal often hinge on the particulars of one or more of those factors. For example, in the context of *jus ad bellum*, debate centers on whether a cyberattack equates to a *use of* *force* or an *armed attack.*[41] Some argue that the determination hinges on the consequences of the cyberattack rather than the instrument of attack itself.[42] However, language in the United Nations Charter involves the manner of attack, as it was written prior to the emergence of cyberattacks when military force between state actors presented the primary threat of concern. Some argue that if cyberattack effects resemble those of other military force generally considered *armed attack*, then the cyberattack will likely be considered an armed attack. Similarly, if cyberattack effects resemble those of harmful actions (political, economic, or covert) that do not otherwise rise to the level of *use of force*, then the cyberattack will not likely be considered such.[43]

Additionally, difficulties with clear attribution complicate these judgments. Absent strong cyberattack precedent, it remains unclear how various actors will apply the principles and how such norms will evolve over time.[44] These issues become further convoluted when they involve non-state actors. While certain international law addresses actions by these groups, traditional law of armed conflict (LOAC) focuses on state-on-state engagement.[45] It seems plausible that some attackers will exploit this ambiguity to conduct cyberattacks in a manner they perceive to reside just below the thresholds of LOAC.[46]

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 cyberattack 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 cyberattacks and their associated effects.[47] Ethical norms based on religious values, ethnic cultures, local traditions, and other factors will vary across international actors.[48] Furthermore, regardless of how clearly or consistently actors apply LOAC, the spectrum of cyberattacks includes a huge range of activity. Much (if not most) of this activity will never rise to the level of armed conflict. While other law including the Convention on Cybercrime, human rights law, and various national laws may apply, evolving international norms will guide how expansive or restrictive cyberattack standards become.[49] 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.[50]

In addition to legal and ethical considerations, actors will also judge whether cyberattack in general and a specific kind in particular seems prudent. Indeed, actors may deem a cyberattack illegal and unethical and still judge it worth doing. A number of factors may make cyberattack an appealing option. Cyberattack may provide an asymmetric capability against an otherwise superior adversary. Traditional warfare can be costly in terms of treasure, lives, and political capital.[51] The low cost of entry for cyberattack allows smaller, poorer states as well as non-state actors a seat at the table. The complexity and costs of certain high-end cyberattack 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.[52] Additionally, anonymity seems useful and achievable via cyberattack.[53] Finally, cyberattack may offer the best—and perhaps only—option for achieving certain effects.

Correspondingly, a variety of factors may dissuade an actor. Cyberattack may not offer a viable solution, at least not with the desired effect and reliability. Such activity may prove politically difficult with either internal or external audiences. Cyberattack may pose unacceptable harmful consequences to others or oneself.[54] An attacker may not want to bear the associated risk of retribution or escalation. Finally, the would-be attacker may not possess the technical capability to reliably plan or execute the desired cyberattack. Evaluation of opportunities and risks as well as the associated benefits and costs will vary across actors and circumstances. However, how a particular actor perceives, weighs, and judges legal, ethical, and prudential considerations will guide its determination of the appropriate circumstances in which to conduct cyberattacks.

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 clear policy on cyberattack.[55] 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 to the many more detailed operational, technical, and organizational issues that follow from them.

Context

To the extent that prevailing U.S. thinking on cyberattack 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 cyberattacks to execute relatively familiar tasks and on certain elements of cybersecurity. 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 cyberattack activities.[56] This territory offers the greatest promise of meaningful cyberattack theory that should form the basis of U.S. policy and strategy going forward (see Figure 2).[57] Technology alone—especially while rapidly changing—cannot provide this foundation.[58] Theory and technology should jointly drive doctrine, and the national guidance under which it is employed.[59]

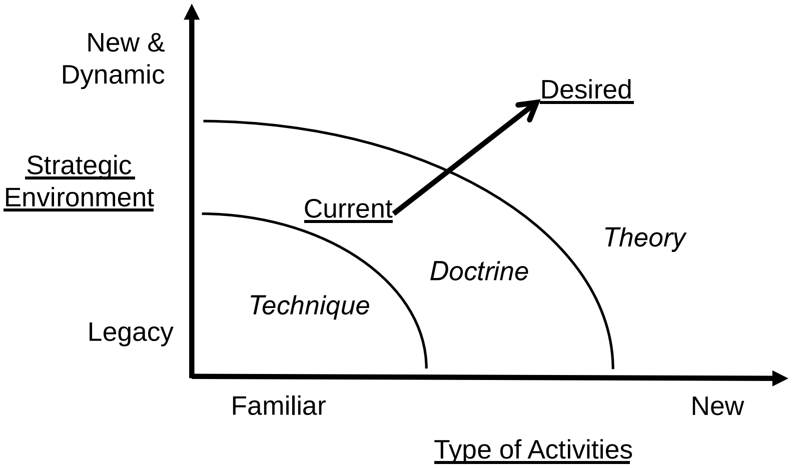

Figure 2. Current and Desired U.S. Contextual Views of Cyberattack Spectrum

Such theory would almost certainly steer policymakers and strategists to a wide-spectrum view of cyberattack. Distinctions between categories of cyberattacks such as war, terrorism, crime, and espionage—and the actors who conduct them—continue to blur.[60] Further, the actions required to conduct or respond to cyberattack will increasingly involve more coordinated participation by military, civilian government, private sector, and international entities.[61] Consequently, U.S. policy and strategy should address a broad range of cyberattacks, including cyber-to-cyber, noncyber-to-cyber, and cyber-to-physical. The latter category will gain increasing importance as "critical mass" is achieved in automation, robotics, and machine learning.[62] 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 cyberattack theory and proclivity to operate within established realms of activity. However, the United States would benefit more from a distribution of effort weighted 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, cyberattack 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 non-state 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 cyberattack technology, the United States should adopt a future-oriented perspective. Better to be constrained by technology than ideas. Finally, policymakers and strategists should devote concerted effort on the linkage between the direct effects of cyberattack and the desired political, security, and economic outcomes, a key element of more mature theory.[63]

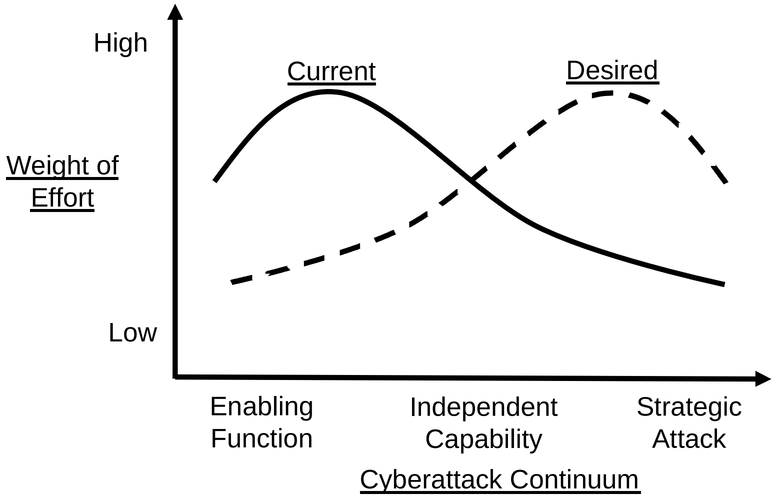

Figure 3. Current and Desired U.S. Balance of Focus

Circumstances

Determining the appropriate circumstances in which to conduct cyberattack may prove illusive; however, it could also produce the most direct consequences. Nobel laureate Thomas Schelling wrote, “One of the lamentable principles of human productivity is that it is easier to destroy than to create.”[64] With that in mind, 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 big of a role will the United States play in what they change to?

Superpower status, allure as a target, and cyberattack 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.[65] 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 cyberattack. 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 cyberattack.[66]

Washington should maintain stability and order by limiting cyberattacks 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: So when does it make sense to conduct, or at least threaten, cyberattack? Assuming that a particular cyberattack is feasible (i.e., it can be done), U.S. policymakers and strategists should evaluate its suitability and acceptability. Suitability addresses causal linkages between a given cyberattack and desired outcomes. In other words, using the logic of cyberattack, one should explain how the particular attack results not just in the direct effects, but also in the desired modification to environmental conditions or adversarial behavior.[67] To inform such evaluations, especially in the absence of sufficient empirical case studies, one needs sound theory that addresses how to impose, defend, deny, coerce, compel, and deter vis-à-vis cyberattack.[68]

If cyberattack offers a suitable option, one should assess its acceptability. Acceptability addresses the conditions created by a cyberattack. 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 cyberattack 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?[69] 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 cyberattack acceptable to the United States? To the international community?

These questions address normative legal, ethical, and prudential aspects of cyberattack that should guide U.S. policy and strategy, but answering them is hard. Joseph Nye, former dean of Harvard's Kennedy School of Government, wrote, "Governments learn slowly from knowledge, study, and experience, and learning occurs internationally when new knowledge gradually redefines the content of national interests and leads to new policies."[70] 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 cyberattack theory, distinct understanding of the cyberattack spectrum, and appropriately weighted effort along the cyberattack continuum.

Conclusion

National governments do not yet have well-defined cyberattack policies and strategies, a condition exacerbated by accelerating changes in power distribution, cyber technology, and other dynamics of the strategic environment. Contextual views of cyberattack, the cyberattack 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 new, dynamic strategic environment in which they occur should form the impetus for developing more comprehensive cyberattack theory. Additionally, a wide-spectrum view that takes a more nuanced approach to categorizing cyberattacks combined with a focus toward the strategic attack end of the cyberattack continuum will properly shape U.S. perspective. Consequently, such perspective will inform a normative approach for determining the appropriate circumstances in which to conduct cyberattack, which will guide both U.S. action and modernization of international norms. The journey to open, distinct, and explicit cyberattack 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.

Endnotes

[1] P.R.C. Groves, *Behind the Smoke Screen* (London: Faber and Faber Limited, 1934), 312, quoted in "Quotations on Airpower," http://www.afa.org/quotes/quotes.pdf (accessed February 7, 2013).

[2] Franklin D. Kramer, Stuart H. Starr, and Larry K. Wentz, *Towards a (Preliminary) Theory of Cyberpower* (Washington, DC: National Defense University, June 2008), 22-26,

http://www.dtic.mil/dtic/tr/fulltext/u2/a486839.pdf (accessed October 11, 2012); Joseph S. Nye Jr., *The Future of Power* (New York: Public Affairs, 2011), 122.

[3] 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: The National Academies Press, 2009), 59, https://download.nap.edu/catalog.php?record_id=12651 (accessed February 18, 2013).

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

[5] 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.

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

[7] Nye, *The Future of Power*, 122-124.

[8] Greg Rattray, Chris Evans, and Jason Healy, "Chapter V: American Security in the Cyber Commons," in *Contested Commons: The Future of American Power in a Multipolar World*, eds. Abraham M. Denwmark and James Mulvenon (Center for a New American Security, January 2010), 143, http://www.cnas.org/files/documents/publications/CNAS%20Contested%20Commons_1.pdf (accessed October 11, 2012).

[9] Eliot A. Cohen, "The mystique of U.S. air power," *Foreign Affairs* 73, (January 1994): 109-124, in EBSCOhost (accessed March 11, 2013).

[10] 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 1900-2006. While not a focus of their work, cyberattack could play an important role in such resistance as a nonviolent (i.e., 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.

[11] Nye, *The Future of Power*, 113-122. Nye writes, "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).

[12] 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 CyberAttacks: Informing Strategies and Developing Options for U.S. Policy* (Washington, DC: The National Academies Press, 2010), 173-176, http://www.nap.edu/catalog/12997.html (accessed January 7, 2013).

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

[14] Milan Vego, “On Military Theory,” *Joint Force Quarterly*, no. 62 (3rd Quarter 2011): 60, http://www.ndu.edu/press/lib/images/jfq-62/JFQ62_59-67_Vego.pdf (accessed February 25, 2013).

[15] James M. Dubik, “Introduction: Get On with It,” in *Rethinking the Principles of War*, ed. Anthony McIvor (Annapolis, MD: Naval Institute Press, 2005), 1-2.

[16] Nye, *The Future of Power*, 144; Clark, *Cyber War*, 197-200.

[17] Martin C. Libicki, *Cyberdeterrence and Cyberwar* (Santa Monica, CA: RAND Corporation, 2009), 117, http://www.rand.org/multimedia/video/2012/02/22/cyberdeterrence-cyberwar.html (accessed February 21, 2013).

[18] Gregory Rattray and Jason Healy, “Categorizing and Understanding Offensive Cyber Capabilities and Their Use,” in *Proceedings of a Workshop on Deterring CyberAttacks: Informing Strategies and Developing Options for U.S. Policy* (Washington, DC: The National Academies Press, 2010), 80, http://www.nap.edu/catalog/12997.html (accessed January 7, 2013).

[19] Ibid., 81-83. Rattray and Healy use twelve 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 non-state actors for political purposes” (77).

[20] Ibid., 82.

[21] Ibid.

[22] Greg Rattray, *Strategic Warfare in Cyberspace* (Cambridge, MA: The MIT Press, 2001), 18. Rattray’s PhD dissertation upon which this book is based (“Strategic Information Warfare: Challenges of the United States,” (The Fletcher School of Law and Diplomacy, May 1998)) can be found at http://www.dtic.mil/cgi-bin/GetTRDoc?Location=U2&doc=GetTRDoc.pdf&AD=ADA346502 (accessed October 11, 2012).

[23] Rattray and Healy, “Categorizing and Understanding Offensive Cyber,” 82.

[24] Clark and Knake, *Cyber War*, 197-200.

[25] John Rollins and Clay Wilson, *Terrorist Capabilities for Cyberattack: Overview and Policy Issues* (Washington, DC: Library of Congress, Congressional Research Service, January 22, 2007), 3, http://www.fas.org/sgp/crs/terror/RL33123.pdf (accessed February 25, 2013).

[26] 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.

[27] Schmitt, “Cyber Operations in International Law,” 156-157.

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

[29] Libicki, *Cyberdeterrence and Cyberwar*, 75-90.

[30] Rattray and Healy, "Categorizing and Understanding Offensive Cyber," 82.

[31] Rollins and Wilson, *Terrorist Capabilities for Cyberattack*, 19-25.

[32] Libicki, *Cyberdeterrence and Cyberwar*, 140-141.

[33] Ibid., 86-91.

[34] Rattray, *Strategic Warfare in Cyberspace*, 14.

[35] Andrew F. Krepinevich, *Cyber Warfare: A "Nuclear Option"?* (Washington, DC: Center for Strategic and Budgetary Assessments, 2012), 62-65, http://www.csbaonline.org/wp-content/uploads/2012/08/CSBA_Cyber_Warfare_For_Web_1.pdf (accessed September 2, 2012).

[36] Rosemary M. Carter, Brent Feick, and Roy C. Undersander, "Offensive Cyber for the Joint Force Commander: It's Not That Different," *Joint Force Quarterly*, no. 66 (3rd Quarter 2012): 22.

[37] Giulio Douhet, *The Command of the Air*, trans. Dino Ferrari (1942; repr., Washington, DC: U.S. Government Printing Office, 1998), 180, http://www.afhso.af.mil/shared/media/document/AFD-100924-017.pdf (accessed March 8, 2013).

[38] Clark and Knake, *Cyber War*, 30-31.

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

[40] Rattray, *Strategic Warfare in Cyberspace*, 120.

[41] Justice of war, or the morality of the conflict itself. As opposed to *jus in bello*, justice in warfare, or ethical conduct within an existing conflict.

[42] Owens, Dam, and Lin, *Technology, Policy, Law, and Ethics*, 251-252.

[43] Ibid., 272. Also, NATO's Cooperative Cyber Defence Centre of Excellence has produced the draft *Tallinn Manual*, a collective effort of experts to determine how existing law of armed conflict applies to cyberattacks; however, this document reflects personal or collective views, but not necessarily views of states. It is not binding, nor does it set precedent. http://www.ccdcoe.org/249.html (accessed February 19, 2013). See also Harold Hongju Koh, "International Law in Cyberspace: Remarks of Harold Koh," *Harvard International Law Journal Online* 54 (December 2012), http://www.harvardilj.org/2012/12/online_54_koh/ (accessed March 8, 2013); and Michael N. Schmitt, "International Law in Cyberspace: The Koh Speech and Tallinn Manual Juxtaposed," *Harvard International Law Journal Online* 54 (December 2012), http://www.harvardilj.org/2012/12/online-articles-online_54_schmitt/ (accessed March 8, 2013).

[44] Ibid., 262-272.

[45] Ibid., 273-277.

[46] Rattray and Healy, “Categorizing and Understanding Offensive Cyber,” 89-90.

[47] Martin C. Libicki, *Crisis and Escalation in Cyberspace* (Santa Monica, CA: RAND Corporation, 2012), 29-35, http://www.rand.org/content/dam/rand/pubs/monographs/2012/RAND_MG1215.pdf (accessed February 21, 2013).

[48] Owens, Dam, and Lin, *Technology, Policy, Law, and Ethics*, 240.

[49] Ibid., 277-282.

[50] Schmitt, “Cyber Operations in International Law,” 177.

[51] Daniel Wagner and John Margeson, “The Globalization of Covert Action,” *Huffington Post Online*, September 9, 2012, http://www.huffingtonpost.com/daniel-wagner/globalization-of-covert-action_b_1869134.html (accessed March 10, 2013).

[52] Nye, *The Future of Power*, 117, 124-125; Rattray, *Strategic Warfare in Cyberspace*, 464.

[53] Martin C. Libicki, “The Specter of Non-obvious Warfare,” *Strategic Studies Quarterly* 6, no. 3 (Fall 2012): 91-92, http://www.au.af.mil/au/ssq/2012/fall/fall12.pdf (accessed September 13, 2013).

[54] Owens, Dam, and Lin, *Technology, Policy, Law, and Ethics*, 241.

[55] For example, see Owens, Dam, and Lin, *Technology, Policy, Law, and Ethics*, 57-62; Clark and Knake, *Cyber War*, 261-264.

[56] Joseph S. Nye Jr., “Nuclear Lessons for Cyber?,” *Strategic Studies Quarterly* 5, no. 4 (Winter 2011): 18, 23, 36, http://www.au.af.mil/au/ssq/2011/winter/winter11.pdf (accessed October 4, 2012).

[57] Vego, “On Military Theory,” 60; Clark and Knake, *Cyber War*, 151-155.

[58] Nye, “Nuclear Lessons for Cyber?,” 24-25.

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

[60] Nye, *The Future of Power*, 144-145.

[61] Nye, “Nuclear Lessons for Cyber?,” 26-29, 36.

[62] Bill Gates, “A Robot in Every Home,” *Scientific American Online*, December 16, 2006, http://www.scientificamerican.com/article.cfm?id=a-robot-in-every-home (accessed March 3, 2013); Peter W. Singer, *Wired for War* (New York: The Penguin Press, 2009), 7-11.

[63] Rattray, *Strategic Warfare in Cyberspace*, 120.

[64] Schelling, *Arms and Influence*, xiii.

[65] Ibid., 153-168. Schelling discusses the conditions conducive for *precedent* to become *norm*.

[66] Schmitt, “Cyber Operations in International Law,” 177-178.

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

[68] Schelling, *Arms and Influence*, 4-5, 69-78; Nye, “Nuclear Lessons for Cyber?” 25-26. Cyberattack could be the method (e.g., a cyberattack to compel adversary action) or the object (e.g., deter cyberattack by the adversary). Also, cyberattack could be conducted alone or in conjunction with other instruments such as economic sanctions and kinetic strikes.

[69] Clark and Knake, *Cyber War*, 197-209.

[70] Nye, “Nuclear lessons for cyber?,” 19.