OXFORD
UNIVERSITY PRESS
Journal of Cybersecurity

An evolving research agenda in cyber policy and security

Journal:	*Journal of Cybersecurity*
Manuscript ID:	Draft
Manuscript Type:	Research paper
Date Submitted by the Author:	n/a
Complete List of Authors:	Lin, Herbert; Stanford University, Center for International Security and Cooperation/Hoover Institution
Subject Specialities:	Subject Six Legal aspects of cybersecurity, Subject Seven: Political and policy perspectives, Subject nine: Strategy and international relations
Keywords:	national security, cybersecurity, policy, law, international relations

An Evolving Research Agenda in Cyber Policy and Security[1]

Herbert Lin
herblin@stanford.edu

May 9, 2015

[1] I gratefully acknowledge comments of various colleagues, including Amy Zegart, Lynn Eden, Richard Betts, Joseph Nye, Susan Landau, Sameer Bhalotra, Judith Reppy, Igor Mikolic-Torreira, and Jack Goldsmith. Obviously, the views expressed in this paper are my own.

This paper presumes some familiarity with the basics of cybersecurity. Those without such a familiarity may wish to consult Appendix A, which is a primer on said basics.

1. Scoping the field of cyber policy and security

The most narrow perspective on cybersecurity as a research field is that it is a mostly technical (i.e., based on computer science, mathematics, and electrical engineering) endeavor aimed at frustrating the actions of a malevolent actor against an information technology system.[2]

A somewhat broader perspective is found in a report of the National Research Council describing cybersecurity as being about "technologies, processes, and policies that help to prevent and/or reduce the negative impact . . . that can happen as the result of deliberate actions against information technology by a hostile or malevolent actor."[3] By implication, research in cybersecurity is with this definition aimed at discovering and inventing new knowledge about such technologies, processes, and policies. Note that this definition acknowledges the importance of processes and policies as well as technologies. Effective and useful policies and processes are grounded in perspectives from many other nontechnical disciplines, such as economics, psychology, organization, and law. In practice, these disciplines are highly relevant to deploying and using solutions that might be developed through technical work and thus must be considered a necessary complement to that work.

A still broader context for work in cybersecurity is that of policy—that is, national and societal interests in preventing and/or reducing the negative impact of events in cyberspace that can happen as the result of deliberate actions against information technology by a malevolent actor. Policy is relevant because certain terms in this sentence are subject to interpretation—the meaning of "impact," on what makes impact "negative," and what makes an actor "malevolent." These definitions are societal constructs, and policy is the name we give to processes for developing these constructions. And, of course, who decides what these terms mean is a central political issue,[4] since the nature of the problem and the potential solutions look different depending on where one stands: one stakeholder's solutions could well be another's problems.

[2] An even narrower view of cybersecurity is that which is done by technicians, network administrators, IT help desks, and other IT workers to help secure individual and enterprise computing facilities. Such individuals install security patches, remove viruses, and undertake other such activities. These activities are important, but they do not constitute research in the usual sense of the term.

[3] National Research Council, *At the Nexus of Cybersecurity and Public Policy: Some Basic Concepts and Issues,* David Clark, Thomas Berson, and Herbert Lin (eds.), National Academies Press, Washington D.C., 2014.

[4] Thomas Hobbes wrote in 1651 that the greatest instrument of political authority is the ability to give names and enforce definitions, so this point is hardly a new one. (Thomas Hobbes, *Leviathan*)

Surrounding cyber policy and security is a cluster of issues that include security but also matters such as correctness, reliability, privacy, safety, and survivability—all of which are attributes or design goals of significance to system developers and operators. Of ultimate concern for trustworthiness is how people perceive and engage with a system, and it is thus the case that unexpected behavior of a computer system works to undermine trustworthiness in multiple ways.

Trustworthiness relates to trust, but they are not the same. Trust is a human phenomenon—it is human beings who do or do not place trust in organizations or technologies. By contrast, trustworthiness is a property of an organization or technology, and provides some of the justification for human beings to trust the organization or technology in question. Human beings may place their trust in technologies or organizations that are untrustworthy, and decision makers or citizens who do so may find themselves at the mercy of technologies or organizations that fail in unexpected ways at inopportune times. Thus, trust and trustworthiness are intricately bound up in issues of security. Trust is also integrally tied to what happens in the future.

Lastly, a rubric of cyber governance and emergence covers the fact that decisions to deploy and use computer systems are based on a belief (i.e., trust) that such deployment and use will be beneficial. But this is not necessarily the case. Computer systems are developed to solve one problem (and may in fact do so), but at the same time they may also create or exacerbate problems or produce unexpected benefits over time. How does a society feel about and manage and govern future worlds in which the “old” problems may be solved more effectively or less expensively but in which a variety of “new” problems manifest and develop over the course of years? Such issues are greatly exacerbated by the possibility of emergence—the deployment and use of various computer systems on a wide scale may interact in ways with each other and with an existing societal infrastructure in ways that no one can predict at the outset.

This paper is focused on cyber policy and security, but the above discussion of trustworthiness, governance, and emergence is provided to place cyber policy and security in an appropriate context.

2. Characterizing research problems in cyber policy and security

Problems in cyber policy and security pose many challenges that are worthy of research. Some specifics are provided below, but first it is helpful consider the nature of these problems from a more abstract perspective. These problems share several characteristics.

- Problems in cyber policy and security generally require multidisciplinary thought and expertise. Of course, some knowledge of the technical fundamentals is necessary (more on this point below). But because of the ubiquity of information technology in nearly all aspects of modern human endeavor, the other disciplines used to understand these aspects are relevant as well. Thus, problems in cyber policy and security often require knowledge from some combination of economics, psychology, sociology, anthropology, law, organizational theory, engineering, political science, and government, among others.

- Problems in cyber policy and security are themselves embedded in a milieu of rapid technological change. Though the fundamental principles of information technology change slowly, new information technology applications are quick to appear. Every new application is an opportunity for cyber mischief—or worse—and thus the relevant context of any problem in cyber policy and security is highly dynamic. Rapidity also characterizes many societal changes that are driven by technology.[5] Examples of such change include changes in the societal meaning of "ownership" and "fair use" in the context of digital distribution of many copyrighted works; changes in concepts of privacy amidst the pervasive use of social media; and changes in what counts as acceptable surveillance amidst the growing ability of both government and private organizations to collect data on an unprecedented scale. This evolving social context makes it difficult to establish cyber policy even when the technical issues are not in question.

- What is known from history and experience—that is, the metaphors, analogies, and precedents with which policy makers are familiar—may break down when applied to the cyber domain.[6] For example, a nuclear analogy for cyber policy and security is tempting, and brings to mind many ideas that can be used for understanding problems in cyber policy and security. Although there are a number of useful analogies between the nuclear and cyber domains, these analogies are not necessarily those that one might first imagine, and may not provide useful guidance for very long. In many cases, the most that can be said about the relevance of these other domains is that many important questions arise in both cyber and the "other" domain (hence knowledge of the "other" domain is helpful), but most answers to these questions are very different (hence one should not push the analogy beyond the point of reasonable utility). In the nuclear case, questions about scale of effect, attribution, strategic and tactical warning, attack assessment, pre-emption, retaliation, and damage-limiting attack planning, reconstitution and recovery, and command and control are central to understanding a number of important scenarios in nuclear conflict. Such questions are also important in cyber conflict—but the nature of the answers to these questions is dramatically different.

- The framing of problems in cyber policy and security profoundly affects how one might approach solutions. For example, many problems can be viewed from national security

[5] I am grateful to Igor Mikolic-Torreira of the RAND Corporation for this point and the examples that follow.

[6] A wonderful collection of analogies for cyber problems and issues is Emily Goldman and John Arquilla, *Cyber Analogies*, Naval Postgraduate School, Monterey, CA, 2014. http://calhoun.nps.edu/bitstream/handle/10945/40037/NPS-DA-14-001.pdf?sequence=1.

perspectives, environmental perspectives, constitutional law perspectives, law enforcement perspectives, perspectives from civil rights and liberties. Each of these fields has its own distinct set of problem-solving tools and intellectual approaches, and the tools and approaches of one field may provide advantages (and disadvantages) as contrasted to those of another field. As an example, much of the concern resulting from the Snowden disclosures has focused on the tension between national security and 4th Amendment rights.[7] Of course, these issues are important, but any resolution of this problem is also likely to have effects on the long-term international competitiveness of the U.S. information technology industry.

3. Identifying "good" and "important" problems in cyber policy and security

What makes a good research problem in cyber policy and security? From an academic research perspective, the traditional answer is a reasonable place to start—A good problem is one that is new, whose analysis provides new, important, and relevant insight and knowledge, and leads to the development of important knowledge over time, and to more good problems.

From a policy perspective, an important problem is one that is relevant to the concerns of the policy maker and that addresses a known or future issue. In this context, consider three distinct categories of relevance.

- Category A—problems whose relevance is known to the policy maker and for which the policy maker needs solutions. Research on Category A problems often develops new solutions, critiques existing solutions, or even reframes known problems from new or different perspectives. These problems also include problems with solutions that are not as effective as they may seem or as conventional wisdom believes. For example, pointing out non-

A rich universe of research problems is only one element of a comprehensive program on cyber policy and security, though it is undeniably critical. Two other critical elements include education and outreach.

Education involves a variety of opportunities for individuals to learn about cyber policy and security at a variety of different levels of involvement and intensity, including 30-minute podcasts or lectures on video; week-long boot camps; course modules to be introduced into other courses; semester-length courses (online and in-class); and thesis projects at the bachelor's, master's, and doctoral levels.

Outreach involves efforts to promote discussion and understanding among parties with different views. Even if these efforts do not result in the solution of specific problems, they can enhance mutual understanding that can be helpful in managing future disagreements.

[7] Again, I am grateful to Igor Mikolic-Torreira for this point.

obvious weaknesses, unintended consequences, or perverse incentives in seemingly obvious solutions falls into this category of research.

- Category B—problems whose relevance to the policy maker is not known or understood today but which should be relevant or which may become relevant at some point in the future. Research on Category B problems often explicates the nature of such problems and explains why they should be important to a policy maker.

- Category C—problems whose relevance is known to the policy maker and for which solutions are already known but may not be remembered or otherwise used. Analyses of Category C problems often remind the policy maker of knowledge that is known in principle but has been ignored or forgotten.

Cutting across all of these categories is an additional theme—the production of new knowledge should also include integration of existing knowledge. That is, papers that integrate existing knowledge—quite possibly from different fields—in new and useful ways can also count as significant research.

Lastly, it should be possible to make meaningful progress on good and important problems in a reasonable amount of time. Thus, an important issue is the extent to which those working on a particular problem can draw on prior background and expertise that might be relevant. For example, cyber researchers wishing to work on problems related to cybersecurity in the financial sector would find their work much easier if they (or their home institutions) have good intellectual and substantive connections to firms providing financial services. Those working on the psychology of decision making during a cyber crisis would benefit greatly from experience with decision making during crises involving other situations characterized by time urgency, severe information gaps, and high degrees of uncertainty.

4. On the Technical Background Needed for Research on Cyber Policy and Security

Technically oriented research in cybersecurity usually does require significant background in computer science, mathematics, or electrical engineering. Many would-be researchers of topics in cyber policy and security extrapolate from this point to express concerns that they do not have the technical background needed to pursue serious research in the field.

But just as few of the people who formulated nuclear strategy and doctrine over the past several decades have known in detail how nuclear weapons work, it is essentially a myth that cyber policy is a field that is primarily technical or that it necessarily requires a degree in computer science or communications engineering. The amount of such knowledge needed for many important problems in research in cyber *policy* is nowhere as much as is often believed, and for many such problems, the necessary technical knowledge about cyberspace, information technology, and cybersecurity—judiciously applied with reason and logic—can be found a variety of publications targeted at nontechnical audiences.

Two useful references that will provide much of necessary technical background—set in the policy context mentioned above—are the National Research Council's *At the Nexus of Cybersecurity and Public Policy: Some Basic Concepts and Issues* and Singer and Friedman's *Cybersecurity and Cyberwar: What Everyone Needs to Know*.[8] Neither will make one a cybersecurity expert, but either (or both) will go some way towards providing the necessary technical background for serious cyber policy research.

The flip side of the comments above is that many important problems in cyber policy do depend on a good grasp of the technical details involved. One important class of such problems involves understanding the policy implications of specific agreements between potentially adversarial parties that involve technical matters. Law and regulation are an instance of such problems—the parties involved in such problems have strong incentives to interpret the precise text of law or regulation in question in ways that favor their own interests—a process known popularly as "finding loopholes." Indeed, the parties involved often hope that their counterparts of the other side will lack the technical sophistication to understand fully the implications of any proposal that they favor.

5. Doing Open Research on a Highly Classified Subject

Another issue often facing would-be researchers in cyber policy and security is that of information unavailability, especially as the result of classification. A substantial amount of policy research on military and defense issues during the Cold War was based on the availability of large quantities of information about the military forces of various nations—capabilities of individual weapons; force structure, leadership, training, doctrine, and so on. The same cannot be said about cyber policy or security, where much of the relevant information regarding the cyber policy of the United States, for example, remains behind closed doors.

Despite this disadvantage, it is still possible to do good and meaningful research on many problems in cyber policy for a number of reasons. First, the U.S. government is slowly releasing more information about matters such as cyber policy and doctrine through various speeches and documents. (The pace of releasing such information is arguably similar to the pace at which the U.S. government released information about nuclear weapons and policy in the early days of the Cold War.) The news media are also more sensitive to the importance of these matters and are another important source of information. Researchers must keep in mind that officially released information about U.S. government thinking about cyber policy and security

[8] National Research Council, *At the Nexus of Cybersecurity and Public Policy: Some Basic Concepts and Issues,* David Clark, Thomas Berson, and Herbert Lin (eds.), National Academies Press, Washington D.C., 2014; Peter Singer and Allan Friedman, *Cybersecurity and Cyberwar: What Everyone Needs to Know,* Oxford University Press, Oxford, England, 2014. Due to personal pride of authorship, I confess to a preference for the first volume, which is also shorter, but the Singer/Friedman volume is also a must-read.

is often incomplete or released without an appropriate framing and context, but that danger is always present when trying to develop independent analysis.

Second, what is most sensitive and classified in the United States tends to be information related to offensive uses of cyberspace *by the U.S. government*. How other parties conduct operations in cyberspace *against* U.S. interests (e.g., against the nation, against companies, against individuals) is discussed rather freely under the rubric of cyber defense (or more precisely, cybersecurity in the traditional sense of the term). And so one way of gaining insight into this otherwise-opaque domain is to consider how the United States government might use offensive operations (of the sort that are discussed in the open literature) to further U.S. national interests, whatever they may be.

A related third point is that the people working behind the veil of classification are constrained by the same laws of physics as those in front of the veil. Both parties use the same underlying technologies in very inventive and creative and innovative ways, and a particularly innovative application of technology behind the veil may be quite surprising to those lacking access. But the broad principles governing the operation of information technology are the same, and reliance on the broad principles can go a very long way towards understanding what may be happening on the inside.

Fourth, researchers usually want information that tells what has actually happened rather than what might have been happening, and would-be researchers in cyber policy and security are often deterred by the fact that much data are unavailable. For example, government officials involved in offensive cyber operations are often quite reluctant to talk about their rationales for actions that they may have ordered or taken, or even what specific actions were involved. Officials involved in a particular cyber incident may not be willing to reveal what they knew or know about what happened (or how they know it). Classification limits disclosure of the actual capabilities of specific adversaries, of friendly nations, and of the United States itself. Companies may not share information concerning cyber breaches out of fear that disclosure would have adverse impact on their businesses.

All of these concerns are valid, and they do limit the scope of research that can be undertaken. Nevertheless, it is valuable to conduct analysis focused on plausible but hypothetical scenarios. At root, what makes a scenario plausible is technical feasibility and political or psychological motivation. Technical feasibility is informed by an understanding of the technology fundamentals described in the previous section. Motivation speaks to a plausible rationale for why an actor might undertake any given cyber operation.[9]

[9] Note, however, that plausible does not necessarily equate to rational. The history of cybersecurity is that when the possibility of a cyber threat is first exposed, an inevitable first reaction is “Why would anyone want to do that?” And after some period of time, someone indeed does that—an action that often leads to great consternation to those who have ignored the problem. Furthermore, publicity about this first action often inspires others to think creatively about ways they can use similar actions to their own ends.

One basic reason that such value exists is that the relative paucity of experience in cyberspace as a domain of conflict. As Gregory Rattray and Jason Healey and later Robert Axelrod suggest, we ain't seen nothing yet.[10] Both of these documents present a range of possible analogies cyber conflict—that is, for how cyber conflict might unfold in practice—and the range is much wider than the few exemplars of cyber conflict that we have already experienced.

As a result, the decisions that policy makers will in the future have to make about cyber conflict are likely to involve scenarios or even classes of scenario that have not yet been experienced and for which by definition data are not now available. Research that provides insight on "new" classes of scenario can thus help to orient policy makers in an uncertain and largely uncharted cyber future.

As an aside, analysis of hypothetical scenarios has the same value that Socratic dialog has for lawyers, thought experiments have for physicists, and tabletop exercises have for planners. These pedagogical instruments help the lawyer and the physicist to explore their own intuitions, to identify preconceptions that may or may not be true, to seek out and resolve contradictions, and to see more clearly the limits of their existing knowledge. For planners, tabletop exercises rarely address exactly the situation a policy maker will face in real life, but may help him or her to sharpen a set of intellectual tools with which to think about new situations.

6. Structuring a taxonomy of research problems

Any taxonomy of problems can be structured in many ways, and the choice of a structuring principle any given taxonomy is to a certain extent arbitrary. The broad taxonomy below is structured primarily by field of relevant expertise. That is, application of a given field of expertise to problems in cyber policy and security will help to advance the state of knowledge. (Also, in many cases, the necessary expertise will require a collaboration between experts in multiple fields.) This particular approach to structuring has the major advantage of being friendly to individual researchers who may wish to enter the field of cyber policy and security but are uncertain about how their expertise may be relevant. Everyone knows his or her own expertise, and a list structured according to expertise is much easier for such researchers to peruse.

The astute reader will notice a mismatch of sorts between the major headings (by field of expertise) and a listing of problem areas underneath each field of expertise. Indeed, this document began with the assertion that interesting problems in cyber policy and security are multidisciplinary, and a proper presentation of expertise against problems would be a matrix, in which the rows were various problem areas, the columns various fields of expertise, and an X in

[10] Gregory Rattray and Jason Healey, "Categorizing and Understanding Offensive Cyber Capabilities and Their Use", in National Research Council, *Proceedings of a Workshop on Deterring Cyberattacks: Informing Strategies and Developing Options for U.S. Policy*, National Academies Press, Washington DC, 2010; Robert Axelrod, "A Repertory of Cyber Analogies", in *Cyber Analogies*, Emily Goldman and John Arquilla (eds.), Naval Postgraduate School, Monterey, California, 2014 (Technical Report: NPS-DA-14-001).

the appropriate cell at the intersection of Row i and Column j would indicate the relevance of Field j to Problem are i, and each row would display multiple X's. But this matrix would be very large and hard to display.

In this document, the major headings by expertise are provided primarily for the convenience of the reader with expertise in a given field, and when a problem area is associated with that field, it means that someone with expertise in that field can make significant contributions to better understanding of that problem area. It is NOT meant to imply that researchers with other fields of expertise cannot make important contributions as well.

Readers who don't like this particular structuring are invited to suggest other structurings designed in accordance with the principle of their choice. Some possible alternative principles include structuring according to the most important problems over a given time-frame, say, 10 years; the most "lucrative" problems currently and in the near-future; the type of cyber policy problem posed; or the cyber stakeholder groups involved.

7. An illustrative taxonomy of problems

Individual problem areas below are described with a few paragraphs to explain their importance. However, in the first two listed problem areas (escalation dynamics in cyberspace and active cyber defense), short concept papers (in Appendix B and Appendix C) are provided to explain its importance more fully. These papers are worked examples what makes this problem area important, why it is a useful focus of research; and some sample questions that might form the basis for specific research projects or papers.

These problem areas are not rank ordered by importance. Moreover, in a new field, it is not at all clear that any given ordering by importance would remain stable for very long. For example, importance often varies by the views of the policy makers involved—in many cases, they would regard as the "most important" the problem areas that are most pressing and time-urgent for them. Nonetheless, making significant progress in any of the problem areas described below would be a contribution to better understanding of cyber policy.

7.1 International security and cooperation

As argued in Appendix A, the increasing importance of information and IT to all aspects of society leads directly to the possibility that various parties might seek to gain advantage over their adversaries by using various tools and techniques for taking advantage of certain aspects of cyberspace, that is "conflict in cyberspace" or "cyber conflict." When these parties are nation states, cyber conflict becomes international, by definition, and thus has implications for international security. (International security also includes conflicts arising from terrorist groups with grievances against a nation, and thus there is a potential cyber dimension to terrorist threats.)

Most topics that are traditionally studied under the rubric of international security have a cyber dimension, and a property or characteristic of information technology and the instruments of cyber conflict may have implications for international security as well. The United States (as do other nations) have two security foci on cyberspace. One focus is defensive and addresses the minimization of cyber harms that adversaries can inflict on it. A second focus is offensive and addresses how the use of offensive cyber capabilities can be used as strategic, operational, and tactical instruments of national policy.

7.1.1 Protection in cyberspace

As noted in Appendix A, the offense often has enormous advantages over the defense under many circumstances; passive defense measures are simply inadequate as the sole or even the primary defensive measure. For this reason, policy makers are often drawn to deterrence—a strategy that seeks to dissuade adversaries from launching hostile cyber operations against the nation or its various interests. Deterrence as a protective strategy is based on two ideas—deterrence by denial persuades an adversary not to attack because he will not achieve his goals even if he does attack, while deterrence by punishment persuades an adversary not to attack because he will suffer unacceptable pain if he does attack.

Regarding deterrence, it is an entirely open question as to whether the extension of traditional deterrence principles to cyberspace makes any sense. A comparison of nuclear deterrence and cyber deterrence illustrates the general observation made in Section 2 that similar questions arise in thinking about nuclear and cyber issues but that the answers to these questions are quite different.

The analysis can start the fact that a nuclear attack of even one nuclear weapon is worth deterring. Such a statement reflects the fact that even the smallest possible nuclear attack—an attack involving the detonation of one nuclear weapon—could result in catastrophe. By contrast, not all cyberattacks are noticeable, let alone significant. In testimony on April 14, 2015 to the Senate Armed Services Committee's emerging threats and capabilities subcommittee, Eric Rosenbach, Assistant Secretary of Defense, Homeland Defense and Global Security, noted that the Department of Defense would only get involved with the most serious cyberattacks against the United States—"only that top 2 percent."[11] Put differently, only a few percent of cyberattacks against the United States might be worth deterring—most are not worthy of that effort.

In this context, the February 2015 testimony to the Senate Armed Services Committee of James Clapper, Director of National Intelligence, is also noteworthy. His statement for the record states that:

[11] http://www.defense.gov/news/newsarticle.aspx?id=128587

> "[Although] the unclassified information and communication technology (ICT) networks that support US Government, military, commercial, and social activities remain vulnerable to espionage and/or disruption,. . . the likelihood of a catastrophic attack from any particular actor is remote at this time. Rather than a 'Cyber Armageddon' scenario that debilitates the entire US infrastructure, . . . we foresee an ongoing series of low-to-moderate level cyber attacks from a variety of sources over time, which will impose cumulative costs on US economic competitiveness and national security.[12]

It may be that the nation's deterrence posture is what makes a catastrophic cyberattack remote. But the nature of the posture needed to deter "low-to-moderate" cyber attacks is not yet well-understood, and it may well require whole-of-government participation and engagement.

There are also important differences in the identification of an attack and attribution of that attack. Nuclear explosions are unambiguous, and because only a few nations have nuclear weapons, the possible targets of a retaliatory threat are known to be one of those nations.[13] Not so in cyberspace, where every nation can afford cyberweapons, and most uses of cyberweapons cannot be clearly and rapidly associated with state actions. Nevertheless, it is simply not true that attribution of an attack in cyberspace is impossible. What is hard is *prompt* and *high-confidence* attribution. In practice, it may take a matter of months before high-confidence attribution of a given cyber attack is attained—if a retaliation is to be effected as punishment for such an attack, how and to what extent does it matter if that retaliation is delayed rather than prompt?

Another issue is that of attack assessment. How would the United States know that it was under a serious cyberattack that warranted a national security response? The emphasis must be on the word "serious", because every day the United States is the subject of many cyberattacks. What is the minimum threshold for such an attack to be deemed serious enough to warrant a national security response?

Yet another issue that complicates cyber deterrence centers on the scope and nature of an appropriate retaliatory threat. As a matter of policy, the United States has stated that it reserves the right to use all necessary means—diplomatic, informational, military, and economic—as appropriate and consistent with applicable international law, in order to defend our nation, our allies, our partners, and our interests [in cyberspace].[14] Article 51 of the United Nations Charter provides that "[n]othing in the present Charter shall impair the inherent right of individual or collective self-defense if an armed attack occurs against a member of the United Nations," and the United States has stated that under some circumstances, a cyberattack could

[12] James Clapper, Director of National Intelligence, Statement for the Record: Worldwide Threat Assessment of the US Intelligence Community, Senate Armed Services Committee, February 26, 2015. http://www.dni.gov/files/documents/Unclassified_2015_ATA_SFR_-_SASC_FINAL.pdf

[13] Although subnational groups can in principle pose a nuclear threat, it is not generally believed that they could obtain a nuclear weapon without the deliberate or unwitting assistance of a nuclear power.

[14] http://www.whitehouse.gov/sites/default/files/rss_viewer/international_strategy_for_cyberspace.pdf

indeed constitute an armed attack or a use of force (forbidden under Article 2(4) of the Charter). But none of the cyberattacks that the United States has experienced to date have come anywhere near any reasonable threshold for “armed attack” or even “use of force.”

For hostile cyber activities that do not rise to the threshold of “armed attack” or “use of force,” only measures short of using armed force are permissible under international law. Today, the toughest policy problems with cybersecurity are how to respond to hostile cyber operations that do not rise to the level of this kind of attack—or, for that matter, do not correspond to other terms recognized in international law, such as use of force or armed conflict. This point is discussed later in Section 7.8 on international law.

If deterrence fails, what then? In the nuclear age, a number of strategists saw value in a damage limitation strategy—a response to an attack that would limit the damage that adversaries can inflict through their attacks. Advocates of this strategy thus promoted weapons systems that enabled U.S. nuclear forces to degrade adversary nuclear weapons so that they posed less of a threat to the United States and its allies.

In cyberspace, damage limitation has also been discussed. For example, in an op-ed written in February 2010, former NSA director Mike McConnell wrote that “deterrence is not enough; preemptive strategies might be required before such adversaries launch a devastating cyber-attack. We preempt such groups by degrading, interdicting and eliminating their leadership and capabilities to mount cyber-attacks…” Preemption—sometimes also known as anticipatory self-defense—is the first use of force against an adversary by a nation that has good reason to conclude that the adversary is about to attack and that there is no other alternative that will forestall such an action. Preemption works either by degrading an adversary’s offensive capabilities or persuading the adversary to refrain from launching an attack that is about to be set into motion.

A related concept is disruption. Because an offensive cyber operation usually unfolds over time, there may be opportunities after it starts to disrupt it—if successful, disruption causes the offensive cyber operation to be less effective than it would otherwise be. Disruption can be effected through the defender’s own offensive cyber operations targeting the adversary assets used in the adversary’s operation.

Some of the questions that arise in considering preemption and disruption as protective measures in cyberspace include the following. What combination of technology and tactics, if any, can help to overcome the difficulties of identifying targets whose preemptive or real-time destruction would degrade the forces involved in an attack? What mechanisms would assure access to these targets? What intelligence information would be needed to make the determination that an attack was impending? What countermeasures could an adversary take in advance to forestall the possibility of being preempted or disrupted?

Active cyber defense is still another approach to deal with the limitations of passive defense.[15] The DOD strategy for operating in cyberspace does not describe active cyber defense in any detail, but its conceptual formulation "active cyber defense" (described in Appendix C) could, if read broadly, include any action outside the DOD's organizational span of control, any non-cooperative measure affecting or harming an attacker's IT systems and networks, any proactive measure, or any retaliatory measure, as long as such action was taken for the purpose of defending DOD systems or networks from that attacker. Some of the actions that could in principle be included under the rubric of active cyber defense are actions taken within and outside of the DOD's span of control.

The most controversial action under the rubric of active cyber defense is the idea of hack-back—an offensive action taken against the adversary who itself is mounting an attack. Appendix C addresses some of the legal and policy questions that arise in considering this and other kinds of action that qualify as active cyber defense.

Once conflict breaks out in cyberspace, questions related to escalation dynamics and termination in cyberspace come to the fore.[16] Much of the serious analytical work related to cyber conflict to date focuses on the initial transition from a pre-conflict environment to an environment in which cyber conflict is known to be taking place. Indeed, studies on deterrence of cyber conflict focus primarily on how to make the initial transition as unlikely or difficult as possible. Little work has been done on three key issues: how the initial stages of conflict in cyberspace might evolve or escalate (and what might be done to prevent or deter such escalation); how cyber conflict at any given level might be de-escalated or terminated (and what might be done to facilitate de-escalation or termination); and how cyber conflict might escalate into kinetic conflict (and what might be done to prevent kinetic escalation). Each of these issues is important to policy makers, both in managing a crisis and in preparing for it. Appendix B contains a more detailed discussion.

Arms control, treaties, conventions, codes of conduct, and international norms of security-related behavior in cyberspace are a second topic of broad significance.[17] Although such topics have been explored in other security contexts (e.g., nuclear, biological, chemical weapons, conventional military forces), the special characteristics of cyberspace call into question some of the traditional models for arms control. A few of these special characteristics include the

[15] National Research Council, *At the Nexus of Cybersecurity and Public Policy: Some Basic Concepts and Issues*, David Clark, Thomas Berson, and Herbert Lin (eds.), National Academies Press, Washington D.C., 2014.

[16] See, for example, Herbert Lin, "Escalation Dynamics and Conflict Termination in Cyberspace", *Strategic Studies Quarterly*, Fall 2012, 6(3):46-70, from which much of this discussion is taken. Available at http://www.au.af.mil/au/ssq/2012/fall/lin.pdf,

[17] A discussion of some of the issues associated with cyber arms control can be found in Herbert Lin, "A virtual necessity: Some modest steps toward greater cybersecurity", *Bulletin of the Atomic Scientists*, 68(5), September 2012. Available at http://thebulletin.org/2012/september/virtual-necessity-some-modest-steps-toward-greater-cybersecurity#sthash.ii7rhG3C.dpuf.

intangibility of many cyber weapons (where cyber weapon is an IT-based tool that can cause offensive effects); the individualized nature of many cyber weapons, which are crafted to address specific targets; the technical similarities between cyber espionage against an adversary's information systems (not forbidden under international law) and a cyberattack against those information systems (possibly forbidden by international law); the availability and use of cyber weapons by nonstate actors.

With such factors—and many others—in play, the feasibility of cyber arms control and other measures is still an open question. But the very openness of this question itself poses an interesting and rich research agenda. What kinds of agreements *are* possible? What steps would in fact help to reduce cyber threats and tensions in cyberspace? How would they be verified? What are the interests that need to be addressed in any given agreement? What should be the norms of acceptable national behavior in cyberspace? What, if anything, can be done to reconcile different national perspectives on what constitutes acceptable norms? And what understandings or agreements are possible to help promote such behavior?

7.1.2 Offensive interests in cyberspace

In principle, offensive cyber operations (OCOs) can be an element of many categories of military action. They can be relevant to cyber-only conflict—that is, conflict restricted to the cyber domain—or they can be integrated with other military operations. A recently released document, *The DOD Cyber Strategy,*[18] states that

> "[t]here may be times when the President or the Secretary of Defense may determine that it would be appropriate for the U.S. military to conduct cyber operations to disrupt an adversary's military-related networks or infrastructure so that the U.S. military can protect U.S. interests in an area of operations. For example, the United States military might use cyber operations to terminate an ongoing conflict on U.S. terms, or to disrupt an adversary's military systems to prevent the use of force against U.S. interests."

Offensive cyber operations can be used across a wide range of scenarios, both tactical and strategic. (For purposes of this discussion, OCOs are cyberattacks rather than cyber exploitations.)

- OCO in support of cyber defense. For example, OCOs may be used to eliminate or degrade cyber threat to DOD systems or networks. In this context, they are classified as "Response Actions" taken for defensive purposes, and are have effects outside DOD systems and networks. They must also be "authorized in accordance with the standing rules of engagement and any applicable supplemental rules of engagement", and the effects they create "may rise to the level of use of force" as understood in the UN

[18] http://www.defense.gov/home/features/2015/0415_cyber-strategy/Final_2015_DoD_CYBER_STRATEGY_for_web.pdf.

Charter.[19] "Hack-backs", as discussed above, are a potentially related concept, although the political, legal, and policy differences between the Department of Defense and a private sector actor undertaking the action are enormous.

- OCOs in support of information operations. For example, OCOs could enhance the effectiveness of psychological operations against adversary decision makers; improve operational security by degrading adversary penetrations of friendly networks; or disseminate propaganda.

- OCOs in support of traditional military operations. As noted in *The DOD Cyber Strategy*, OCOs can be used to disrupt adversary command and control networks, military-related critical infrastructure, and weapons capabilities.

For some set of OCOs, it may make sense to consider what a notional cyber tasking order (CTO) might entail. A CTO could be analogous to an air tasking order that specifies at a high level of detail the actions of cyber or air assets in a specific conflict for a specific period of time. For another set of OCOs, a plan for usage might be modeled on what used to be called the SIOP and is now designated OPLAN 8010 for Strategic Deterrence and Global Strike. Such a plan could include a list of targets, a timetable on which these targets are to be attacked, and the cyber-weapons that are to be used in the attack on those targets. It would also provide options intended to create large-scale effects and others to create small-scale effects narrowly tailored to address a particular target set.

As for strategic considerations, a comprehensive strategy for the use of OCOs would include:

- A clear statement of the objectives to be achieved by the possession and possible use of OCOs. One such objective might (or might not) be deterrence of adversary cyberattacks against the United States, its allies, or their interests.

- A description of the possible adversaries that might be the target of OCOs.

- The broad missions that OCOs might serve (e.g., deterrence of cyberattack, deterrence of conventional attack, integration into traditional kinetic military operations)

- The circumstances (broadly described so as not to set precise thresholds) under which these broad missions would be executed. As noted in *The DOD Cyber Strategy*, OCOs may be conducted during periods of heightened tension (i.e., before the outbreak of outright hostilities).

- The force structure needed to execute these missions.

- The impact of offensive cyber capabilities on strategic stability.

[19] Joint Publication JP3-12R, Cyberspace Operations, 2012

- The types of target that might be the focus of OCOs (e.g., nuclear forces, conventional forces, command and control facilities, war-supporting industry, leadership and centers of political power and control) and the kinds of cyber effects that might sought in such targeting (e.g., destruction, denial of service, and so on).
- The development of appropriate standing rules of engagement for using cyber weapons for attack.

A second set of uses for offensive cyber operations relates to the missions of the intelligence community. The use of OCO for cyber exploitation—exfiltration of information for intelligence-gathering purposes—is well known. But a second set of missions of the intelligence community—those related to covert action—receives far less attention. The U.S. Code (50 USC 413b(e)) defines covert action as "an activity or activities of the United States Government to influence political, economic, or military conditions abroad, where it is intended that the role of the United States Government will not be apparent or acknowledged publicly." Cyber weapons for attack well-suited for such a role, and in this context the range of possible missions for cyber weapons is much broader than just military missions. The possible mission space for covert action using cyber weapons for attack includes, for example, influencing an election, instigating conflict between political factions in another nation, harassing disfavored leaders or entities, or diverting money from disfavored factions in another nation.

One more question related to offensive cyber capabilities deals with their export.[20] Many nations, including the United States, sell weapons to other nations, and the U.S. government has a framework known as the International Traffic in Arms Regulations (ITAR) in place to deal with the export of U.S. kinetic to other nations Though these weapons are often kinetic weapons such as missiles, jet fighters, tanks, and ships, there is no reason in principle that these weapons could not be cyber weapons. Other nations have sought to obtain such weapons—or more precisely, offensive cyber capabilities—from the United States. However, the details of any of these attempts to obtain these capabilities are not known publicly. Irrespective of the ITARs per se, what considerations should drive the formulation of policy as related to the export of offensive cyber capabilities to other nations?

7.1.3 Other approaches to cybersecurity

It is a fact that the language of national security is often used to describe the cybersecurity problem. This is not surprising, as cybersecurity *is* a problem of national security. But important questions arise as to whether other paradigms might shed useful light as well. For example, the Center for Internet Epidemiology and Defenses was established to explore the

[20] An interesting paper on this topic by Trey Herr and Paul Rosenzweig can be found at http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2501789.

relevance of epidemiology to cybersecurity.[21] Among the problems addressed by the center: how the Internet's open communications and software vulnerabilities permit worms to propagate; how to devise a global-scale early warning system to detect cyber epidemics in their early stages; the development of forensics capabilities for analyzing wide-ranging infections; and the development of techniques and devices that can suppress outbreaks before they reach pandemic proportions. More recently, Rowe et al developed parallels between public health and cyber security threats and interventions to understand individual risk preferences for cyber security that can help identify the types of interventions and related implementation and communication strategies that will more effectively improve cyber security.[22]

Healey and Pitts suggest that international environmental legal norms also have considerable applicability to cyber security.[23] They argue that international environmental law has been able to assert a significant though limited state liability for certain acts that originate within the territory of one state that cause harm to another state or to its citizens. Applying this norm to cyberspace offers the possibility that states could be held liable for cyber-pollution (that is, hostile cyber actions) emanating from their territory—whether or not the governments of those states were actually encouraging or directing those actions. Thus, state responsibility could be established for both state and non-state actions in cyberspace.

Control and oversight regimes relating to dual-use technologies may provide useful insights as well. For example, biotechnology is a dual-use technology for which many oversight and control mechanisms have been developed, even apart from the Biological Weapons Convention. How and to what extent, if any, are similar mechanisms usable to curb the use of cyber weapons for hostile purposes?

7.1.4 Regional concerns regarding cyber policy and security

A variety of regional concerns in cyber policy and security warrant investigation. For example, many nations in Eurasia (China, Russia, and the other members of the Shanghai Cooperation Organization) have radically different views of what constitutes security in cyberspace. Specifically, they reject the term cybersecurity in favor of “information security”, a conceptualization that allows them to regard as protective mechanisms what the West would see as censorship efforts—in this view, a negative article in the New York Times about a nation’s leadership is regarded as a national security threat just as is an email containing malware in an attachment.

Regional concerns can be divided into at least three broad categories. One category is that of cyber policy and security issues in existing alliances, such as NATO, ANZUS, and so on.

[21] http://www.nsf.gov/news/news_summ.jsp?cntn_id=100434
[22] Rowe, B., Halpern, M., & Lentz, T. (2012). Is a public health framework the cure for cyber security?. CrossTalk, 25 (6):30-38.
[23] Jason Healey and Hannah Pitts, “Applying International Environmental Legal Norms to Cyber Statecraft”, http://moritzlaw.osu.edu/students/groups/is/files/2012/02/6.Healey.Pitts_.pdf

Managing cyber policy and security issues in existing alliances involves reconciling national policies with those of the alliances, a task that is often politically fraught. How, for example, should NATO regard offensive operations in cyberspace as a response option to cyberattacks on NATO networks?

A second category is cyber policy and security issues in specific geographic regions, e.g., the Asian Pacific Rim, Africa, and so on. These regions are interesting because their large) indigenous populations will be coming online—by the hundreds of millions—in the next decade, and adding these populations will inevitably pose new security challenges on the Internet. One broad research topic relevant to this second category is the impact of the limited security capabilities of the mobile devices that the vast majority of these new netizens will use for internet access.

A third category of regional issues is the cyber relationship between near-peer nations, such as the United States and China. These two nation are arguably the two most important nations in the world with respect to information technology, the Internet, and cyberspace. Given that cyberspace and the internet span national boundaries, and that both nations increasingly rely on information technology, it is not surprising that the cyber relationship regarding between China and the United States has both competitive and cooperative aspects.

The competitive aspects of this cyber relationship are well-known, and include differences over economic espionage conducted for the benefit of private companies and the extent to which speech should be regulated by national governments and the proper degree of "openness" on the Internet. Each side is sensitive on these points, in the sense that each feels strongly about them and reacts powerfully when their views on these points are challenged, and so the dialogue between China and the United States has been dominated by differences on such issues. By comparison, the potentially cooperative aspects of the relationship have been neglected. Simply as illustrations, some of these aspects include:

- Chinese and U.S. understanding regarding various cybersecurity-related concepts; knowledge of each nation's laws and policies regarding cyber security and cyberspace and how the current authorities of each nation understand and interpret these laws.

- Understanding the critical thresholds of each nation. Without such understanding, one nation may inadvertently cross a threshold of the other nation and thereby escalate a conflict without intending to do so.

- Methods to reassure the other nation of non-involvement in the event of a cyber disaster or a high-consequence cyberattack by a third party.

- Methods for one nation to assist the other in the event of a cyber disaster or a high-consequence cyberattack by a third party; international management of cybersecurity incidents.

Research into these and other topics might well help to build some foundations for cooperative cyber security between the two nations.

7.2 Cyber Protection of Critical infrastructure[24]

By definition, a nation's critical infrastructure provides the essential services that underpin that nation's society. Presidential Policy Directive 21 (PPD-21) notes that critical infrastructure is diverse and complex, and includes distributed networks, varied organizational structures and operating models (including multinational ownership), interdependent functions and systems in both the physical space and cyberspace, and governance constructs that involve multi-level authorities, responsibilities, and regulations.[25] PPD-21 designates 16 sectors of the economy as critical infrastructure: the chemical sector; commercial facilities; communications; critical manufacturing; dams; the defense industrial base; emergency services; energy; financial services; food and agriculture; government facilities; healthcare and public health; information technology; nuclear reactors, materials, and waste; transportation systems; and water and wastewater systems.

To preserve the functionalities afforded by critical infrastructure, the infrastructure must be secure and able to withstand and rapidly recover from all hazards, including a wide range of possible cyber threats. As in other domains of concern, the security and resilience of critical infrastructure are much more than just technical problems—they have organizational, legal, regulatory, economic, and business dimensions as well.

Consider, for example, the interconnectedness of infrastructures such as the electric power grid or the financial system. Institutions in these large-scale networks depend on one another for their daily operations, and a failure in one institution can have devastating effects on others to which it is connected. Yet senior management at any particular institution, left to their own devices, do not have much incentive to consider taking measures that go beyond protecting against the risk faced by their own institution. That is, they are primarily concerned with taking measures that address their own business risks, and the entire network of interconnected institutions is less protected than any of the individual institutions within the network. Such problems are exacerbated in an era that frowns upon high degrees of direct government regulation.

Interesting questions thus arise about the scope and nature of mechanisms whose deployment and use can improve the security and resilience of large, interconnected, interdependent infrastructures. For example, an important technical question relates to how rapidly the effects of a failure in one institution will propagate through the network to affect others. (A related issue is the design of alternative architectures for these infrastructures that would support

[24] This discussion of scope and nature of critical infrastructure is taken from PPD-21.

[25] https://www.whitehouse.gov/the-press-office/2013/02/12/presidential-policy-directive-critical-infrastructure-security-and-resil

interconnectedness and interdependence of institutions during normal operation and standalone operation when necessary to protect against the propagation of a failure's effects.) An important regulatory question is the extent to which existing regulatory bodies with jurisdiction over the various individual institutions within a network can require those institutions to take measures for security and resilience beyond those needed for the business needs of those individual institutions. An important economic question is how to identify incentives for institutions to take more responsibility for overall network security and resilience.

Another class of questions about critical infrastructure relates to its definition. The 16 sectors designated by the Department of Homeland Security account for a large portion of the U.S. economy—but in the limit, when everything is critical, nothing is critical. So what is truly the critical critical infrastructure? Is it really true that Sony Pictures Entertainment—the victim of a North Korean hack in late 2014—is a part of the U.S. critical infrastructure? (Answer—according to the DHS definition of critical infrastructure, it is.[26]) By what measure should it count as critical infrastructure?

Yet another broad category of issues related to cyber protection of critical infrastructure is that of transition planning from less secure to more secure critical infrastructure. As an example, some analysts foresee the day when the public-key encryption technologies used today (i.e., those based on the RSA algorithm) will be vulnerable to advances in quantum computing. Research is underway to find encryption technologies that will be far less vulnerable to quantum computing, but whatever those technologies are, having in place an orderly transition plan to move from the technologies of today to those of tomorrow would be a great help if and when the current technologies are shown to be incapable of providing adequate protection in light of technological advances. Transition planning would identify and assess issues likely to arise in any contemplated transition and an evaluation of various approaches managing such issues.

7.3 Private sector concerns

Unlike many other dimensions of national security, the private sector is intimately involved with matters related to cybersecurity. Most of the information technology on which we rely is owned and operated by the private sector. A vast majority of the communications of the Department of Defense are carried over private sector telecommunications facilities. So the robustness of the cybersecurity posture of the private sector is a key concern of policy makers.

Some of the issues that fall under this rubric include current good or best practices for cybersecurity that are applicable for private sector needs; the appropriate standards (if any are appropriate) for cybersecurity that different elements of the private sector should follow; and

[26] See http://www.dhs.gov/commercial-facilities-sector, which lists the entertainment and media industry as a part of the Commercial Facilities Sector, which is one of the 16 sectors of the U.S. economy officially designated as critical infrastructure.

how any standards adopted should evolve into the future with technological change and changes in the business and political environment.

The private sector also has an increasingly large appetite for cybersecurity personnel. These individuals are responsible for maintaining and improving the cybersecurity posture of private companies and organizations. How will this appetite be satisfied in the future? What specialized education and training should such personnel have, especially in an environment in which everyone who uses a computer needs to know some of the basics of cybersecurity?

A particularly controversial private sector concern is the use of offensive cyber operations conducted to enhance the cybersecurity posture of the private sector. The Department of Defense reserves the right to undertake offensive cyber operations in response to hostile actions against U.S. military assets in cyberspace. Such operations, sometimes included under the rubric of active defense, are tactical operations whose goal is limited to mitigating the immediate hostile act. If so, why should similar operations not be useful in mitigating a given cyber threat to assets in the private sector or in non-defense parts of the U.S. government? Under current U.S. law and policy, such operations by the private sector to defend their interests in cyberspace are forbidden. What would be the utility and impact of changing current law and policy in this regard? What are the legal and policy issues that such a change would entail? What kinds of offensive cyber operations, if any, that should be undertaken to protect private sector entities? If any should be allowed, who should conduct such operations?

7.4 Economics

At its most basic core, economics is about the study of incentives of various kinds, and thus a natural connection between economics and cybersecurity is the study of incentives to develop and use various technologies, processes, organizational structures, and such to enhance the cybersecurity posture of any given entity, whether an individual, an office, an organization, an industry, or a nation state.[27]

Moore describes several economic factors that affect cybersecurity.

- Misaligned incentives. Systems tend to be more vulnerable if the party responsible for protecting the system can avoid some or all of the costs incurred when the systems fails. For example, in a highly networked system (such as the banking industry or the electric power industry), a failure of one facility or entity may cause system-wide failure—and yet no individual facility or entity bears the cost of the entire failure.

[27] A primer on the economics of cybersecurity is found at Tyler Moore, "Introducing the Economics of Cybersecurity: Principles and Policy Options", in *Proceedings of a Workshop on Deterring CyberAttacks: Informing Strategies and Developing Options for U.S. Policy*, http://www.nap.edu/catalog/12997.html, 2010.

- Information asymmetries. In cybersecurity, the data needed to drive security investment if often absent. For example, there are few estimates of aggregate losses due to cybersecurity breaches and intrusions that are based on defensible methodologies.[28] Measuring the level of cybersecurity protection afforded by any given set of technologies, processes, and procedures remains a matter of intuition and guesswork.

- Externalities. Externalities are present when the decisions of one entity with respect to cybersecurity are affected similar decisions made by others. For example, network externalities mean that a decision to do X makes more sense if many others also do X. When network externalities are present, being the value of being first-to-market increases—and because paying attention to security does not increase the likelihood of being first to market, security is often neglected in initial product or service offerings.

As one example of the above factors at work, the national cybersecurity posture is today significantly less robust than it would be if known security technologies and best practices were deployed and used widely. Thus, some part of the cybersecurity problem lies in persuading or incentivizing organizations and responsible individuals to do so. However, when organizations and individuals do pay attention to cybersecurity, they generally do so as a matter of managing their own risks rather than those of society. Even if the result is adequate for them individually, the overall national cybersecurity posture that results from many such individual investment decisions is lower than the nation needs as a whole.

Recognizing the failure of the free market to deliver a sufficiently robust cybersecurity posture for the nation, both the public and private sector have undertaken initiatives to improve incentives for cybersecurity. But there is still no consensus on what needs to be done, and it remains an important challenge as to how to move forward on using market mechanisms to promote cybersecurity in the absence of a political consensus.

Another example of a deep connection between economics and cybersecurity relates to the role of the cyber insurance market in enhancing cybersecurity. Understanding this connection starts with the realization that in other domains such as fire safety, the insurance industry has an important driver of improvements in safety and security. Building owners needed insurance against catastrophic loss from fire. Underwriters provided policies that provided such insurance, but they lowered their rates if the insured buildings met certain requirements that improved their fire resistance of the insured building. Owners seeking better rates thus made those improvements.

[28] For example, if a company that spent $100 M on research to develop a particular trade secret and that research is stolen, the loss to the company is certainly not $100 M. One reason is that company still has that research to use. What is stolen is the period of time over which the company has a monopoly on that research, and shortening that period of time may cost the company an amount of money that is only weakly related to that original $100 M for research.

Why isn't the same true for the cyber insurance market? Why doesn't the logic in the above paragraph work if one simply replaces "fire" with "cyber threat"? It's true that the cyber insurance market is growing, but what is less clear is the extent to which cybersecurity practices are improving as the result of underwriters' requirements. So an interesting open question is how and to what extent, if any, can cyber insurance underwriters can indeed influence meaningful improvements in cybersecurity.

A third example concerns zero-day vulnerability markets. A zero-day vulnerability (ZDV) refers to a vulnerability for which the responsible party (e.g., the vendor that provides the software) has not provided a fix, often because the vulnerability is not yet known.[29] An intruder can often take advantage of a ZDV before it is fixed; because such vulnerabilities have value, markets have arisen in which these vulnerabilities are bought and sold. Vendors often pay bounties for knowledge of ZDVs so that they can repair them, but ZDVs are also sold to parties who wish to take advantage of them in an intrusion. Understanding these markets is a difficult intellectual task because much of their operation is shrouded in secrecy, and yet such understanding could be valuable in reducing the flow of such vulnerabilities to parties of malign intent.

An economics perspective also helps to inform decisions about how to invest in cybersecurity. Given an additional dollar to invest, where should it be invested to obtain the largest security return? Should a corporate cybersecurity team invest in full-disk encryption or in Lojack (a tracking program) to protect its laptops from theft? Will a corporation's data be more secure in the cloud or in in-house computing? Should the complexity of computing (and thus its functionality) be reduced in a given system to obtain security benefits associated with simplicity? Solutions to such problems are data-intensive, but valuable for security decision makers.

A last example for this paper focuses on the labor economics of cybersecurity. By all accounts, cybersecurity is a "hot" profession today, with significant demand for cybersecurity workers in the U.S. government (including the armed forces) and in the private sector. But what knowledge should cybersecurity workers have? For that matter, what is a cybersecurity workers? Arguably, workers in any occupation in which the use of a computer is required must know some things about cybersecurity—thus, office workers, architects, line workers in highly automated factories, and police officers need to know about cybersecurity. But what these workers need to know about cybersecurity almost surely different in both degree and kind from what cybersecurity researchers in academia and the information technology industry or full-time network administrators need to know.

Furthermore, much cybersecurity work is today labor-intensive, which accounts in part for the profession's "hotness". It is likely that simply training more cybersecurity professionals similar to those that we train today will keep up with the demand. How and to what extent, if any, can human productivity on various aspects of cybersecurity be enhanced through the use of

[29] National Research Council, *At the Nexus of Cybersecurity and Public Policy: Some Basic Concepts and Issues*, David Clark, Thomas Berson, and Herbert Lin (eds.), National Academies Press, Washington D.C., 2014.

technology? The technical side of this is illustrated by the current DARPA Cyber Grand Challenge, which is a competition that seeks to create automatic defensive systems capable of reasoning about flaws, formulating patches, and deploying them on a network in real time.[30] If successful, what will be the impact on the labor market for certain kinds of cybersecurity professional?

7.5 Psychology and Education

Psychology and education are central to many issues in cyber policy and security. Deterrence itself can be regarded as a psychological or an educational problem—deterrence seeks to convince or persuade an adversary that the costs of taking a particular action outweigh the benefits of doing so. Psychology—specifically cognitive psychology and science—are highly relevant to usability studies of security technology and procedures; such studies are key elements in understanding why what is known about cybersecurity is often not applied or used in the field. Cyber hygiene and awareness refers a class of basic actions that users take to enhance their cybersecurity posture—and user education is a critical element of imparting cyber awareness. The psychology of decision making under extreme uncertainty has been studied in contexts such as the Cuban Missile Crisis, but precious little is known about similar decision making in the midst of cyber crisis.

One illustration of a connection between psychology and cyber policy is the psychological effects of cyber warfare. Consider the possibility of an attack that specifically targeted against national confidence. In many scenarios, the target of a hostile cyberattack is often assumed to be the computer systems and networks controlling critical infrastructure such as electric power and banking/financial systems.

Most analytical work addresses the extent to which such an attack might seriously compromise the actual ability of the infrastructure to deliver the services on which the nation relies – and in some sense depends on the ability of the attacker to cause serious damage to important parts of the cyberinfrastructure.   However, an attacker seeking to destroy public confidence in critical infrastructure may not have to cause a great deal of actual damage, and diminished public confidence in systems that have been subject to a serious cyberattack may exceed what would be expected based on the actual effects.

For example, cyberattacks against financial institutions that corrupted only a small number of transactions—or simply created ambiguity as to whether transactions might have been corrupted—could cause a loss of faith in the wider system, with consequent effects on markets. In some cases, the impacts of reduced confidence might greatly exceed that of the actual incident.

[30] http://www.darpa.mil/Our_Work/I2O/Programs/Cyber_Grand_Challenge_%28CGC%29.aspx.

Serious work on the psychological effects of cyber warfare might thus seek a better understanding of the likely public response to cyber events, and a consideration of how the public response to future events could best be observed and analyzed; development of effective strategies for communicating with the public in the event of such a cyber event; and enhanced technical, intelligence, and analytical capabilities that improve the quality of the information available to decision makers.

A second illustration is the issue of the deterrence value of delayed retaliation, mentioned earlier. At least two issues here are salient. First, what discount, if any, should be applied to the deterrence value of a delayed retaliation as compared to a prompt retaliation? In the limit of an infinite delay, the discount is 100%. Further, the value-decay curve as a function of delay time may well differ for different actors. How might such a curve be measured? A second issue is the possibility that with the passage of sufficient time, the victim may not retaliate at all. Furthermore, with the passage of sufficient time, the victim—or the world at large—may come to see an act of retaliation as a new and unprovoked act of aggression. Addressing such issues requires work on human psychology.

7.6 Sociology/Anthropology

According to one common definition easily found on the Internet, sociology focuses on the structure of groups, organizations and societies and how people interact within these contexts. The American Anthropological Association says that anthropology (more specifically, cultural anthropology) focuses on social patterns and practices across cultures. That is, both sociology and anthropology study societies and cultures, and the cyber world contains many distinct societies and cultures of interest.

One culture—more precisely, one set of cultures—worthy of examination is the culture of the hacker. Who are the people who become cyber adversaries? Why did they get involved? What are their motivations? What might trigger them to launch attacks in cyberspace? How do they organize themselves? Answers to these questions might yield useful information that could help identify future threats, discourage people from becoming adversaries, dissuade them from launching attacks, and identify critical nodes in their networks whose targeting might be seriously disruptive to their efforts—and such questions are sociological and anthropological in nature.

A second societal point is that the cyber relationship between nations is embedded in a much larger context that spans their respective histories and cultures. Given such embedding, it would not be surprising if they would bring to the cyber relationship long-standing perspectives and views shaped by non-cyber events.

Such embedding is entirely relevant to the China-U.S. relationship in cyberspace. The discussion in Section 7.1 noted important differences between U.S. and Chinese perspectives on cyberspace. Whether such differences can be bridged remains to be seen, but efforts on both sides to find common ground should at the very least be informed by a mutual understanding of how their narratives regarding cyberspace are shaped by their cultures and histories. Such understanding is not common on either side of this relationship.

Yet another societal and cultural topic of interest concerns generational differences in perceptions of cybersecurity and related issues such as privacy. In many developed nations, the youth of today are "digital natives."[31] These individuals have never known a world without the Internet or ubiquitous information technology at their fingertips—and their sensibilities, values, and perceptions about the digital environment called cyberspace are often different than those of older generations. How and to what extent, if any, will their views on matters such as privacy and security come to shape the future dialog about such matters? Will their ease and familiarity with technology make it easier or harder to improve the safety and security of cyberspace?

7.7 Organizational structure and behavior

Organizational structure and behavior is also a driver of a number of cybersecurity concerns and interests. For example , what makes some organizations more successful than others at coping with the cyber threats they all face? Leadership? Budget? Awareness? Technology? Training? Accountability? Better public relations? How do these and other elements contribute to a stronger cybersecurity posture? (This question does presume that it is possible to know that one organization's cybersecurity posture is better than that of another—despite the possibility that it may be very hard to know, most security analysts have an intuitive sense that not all organizations are in fact equal in this regard.)

Another set of organizational issues relate to military organizations into which cyber weapons are introduced. Such weapons may have significant impact on the practices, procedures, and lines of authority embedded in those organizations, especially if these weapons are as revolutionary as is often claimed.[32] Organizational structure and culture are the foundations of accountability and chains of command, and affect matters such as promotion, respect, levels of cooperation between units, and influence within a hierarchy. Introducing new technology that affords new capabilities often affects the assumptions on which the organization is structured, and thus may have implications for the organization. Two interesting questions include the following:

[31] See, for example, John Palfrey and Urs Gasser, *Born Digital: Understanding the First Generation of Digital Natives*, 2010.

[32] Much of the discussion in this section is adapted from NRC, *Emerging and Readily Available Technologies and National Security: A Framework for Addressing Ethical, Legal, and Societal Issues*, NAP, WDC 2013.

- As a doctrinal matter, the U.S. military has generally chosen an approach to managing its combat forces in a way that places responsibility for execution (how tasks are performed) on lower ranks in the military hierarchy while maintaining centralized command and control (what tasks need to be performed). How and to what extent, if any, do the special characteristics of cyber weapons and their likely targets change the balance that should be struck between centralized command and control and decentralized execution? (For example, how aggressive should U.S. cyber warriors be in penetrating adversary command and control networks if those networks are connected to the adversary's nuclear command and control system?)

- Military organizations often place great value on personal bravery in combat. How and to what extent, if at all, does cyber warfare—in which individuals are not placed in direct physical danger—change such valuation? The DOD's abortive attempt to introduce a Distinguished Warfare Medal in 2013 is instructive in this regard.[33]

Another important organizational dimension of cybersecurity is the role that nongovernmental groups play in enhancing in internet security and resilience. For example, it is well known within the networking community that the successful resolution of many network-based attacks and other operational problems has entailed the involvement of informal technical working groups, brought together on an ad hoc basis and involving network administrators who know each other. Through these working groups, such attacks have often been mitigated and curbed in relatively short times. Such groups are thus an important element of maintaining network security and stable operation. Groups such as the Internet Engineering Task Force play key roles in establishing standards that enable the smooth operation of the Internet and guide its future evolution. Despite the importance of these nongovernmental groups, little is known today about how these groups form and work, the necessary preconditions for the formation of such groups, and what these groups do and do not need from governments and policy makers to continue working effectively.

A final example of organizational issues in cybersecurity involves mechanisms for information sharing. It is widely accepted that some degree of information sharing among victims of cyber intrusions and with the U.S. government would enhance the cybersecurity posture of these organizations and of the United States. One reason is that such information must be pooled to identify a large-scale attack. Also, sharing information could help individual organizations be better prepared to address specific cyber threats. Unfortunately, it is also widely accepted that existing information sharing arrangements have not been fully successful in achieving their goal. Some parties complain that they give information but don't get useful information in return. Others worry about the privacy and civil liberties implications of sharing information with government authorities. What are the barriers to effective information sharing, and what can be done to eliminate or reduce those barriers?

[33] http://www.washingtonpost.com/world/national-security/pentagon-cancels-divisive-distinguished-warfare-medal-for-cyber-ops-drone-strikes/2013/04/15/62335492-a612-11e2-8302-3c7e0ea97057_story.html

7.8 Law

Law as it relates to cyber policy and security comes in two distinct flavors—domestic law and international law.

7.8.1 Domestic Law

The United States has a number of domestic laws that pertain to various aspects of cyber policy and security.[34] Some of the most important are the Computer Fraud and Abuse Act, which addresses unauthorized access to computers; the Electronic Communications Privacy Act, which regulates the conditions under which government surveillance of domestic electronic communications may occur; and the Foreign Intelligence Surveillance Act, which regulates the conditions under which government surveillance of electronic communications for foreign intelligence purposes and involving Americans may occur.

In addition, many domestic laws criminalize various actions without specific regard for the instruments used in such actions. For example, the Economic Espionage Act criminalizes the stealing of economic information without specific mention of how one might effect such a theft; nevertheless, such theft is today often perpetrated through cyber means.

A variety of domestic laws allocate responsibility for different aspects of cybersecurity among different federal agencies, both for the federal government and with respect to much of the private sector. For example, Department of Defense authorities are laid out in Title 10 of the U.S. Code, those of the Intelligence Community in Title 50, those of the Department of Justice in Title 18, those of the National Guard in Title 32 (the National Guard is potentially relevant to cybersecurity at the state level because the Guard responds to state needs and some of its members are civilians with significant IT skills derived from their day jobs in the IT industry), and those of the Department of Homeland Security in Title 6.

Lastly, export control law has long been used to stem the proliferation of certain “dangerous” technologies, that is, technologies that would be dangerous were they to fall into the hands of U.S. adversaries. Under the Arms Export Control Act of 1976 (22 USC 39), the President of the United States has the authority to control the export of defense articles and defense services which are found on the U.S. Munitions List; these articles includes a number of military information security assurance systems and equipment, and cryptographic devices, software, and components specifically intended for military applications. In addition, the Department of Commerce’s Export Administration Regulations apply to “dual-use” technologies, that is, technologies that can be used for either civilian or military purposes, including certain

[34] A comprehensive description of the domestic legal regime can be found in Eric Fischer, *Federal Laws Relating to Cybersecurity: Overview and Discussion of Proposed Revisions*, Congressional Research Service, Washington DC, 2013. Available at https://fas.org/sgp/crs/natsec/R42114.pdf.

technologies related to cybersecurity (certain technologies for cyber defensive purposes and other technologies for cyber offensive purposes).

Statutory law is only one aspect of the domestic legal regime; a second important aspect is the set of executive orders that are issued by the White House and are legally binding on federal agencies. For example, Executive Order 12333 governs the activities of U.S. intelligence agencies, some of which have an important bearing on U.S. surveillance practices.

Many aspects of the existing domestic legal regime are widely viewed as needing to be updated in light of recent developments such as increases in cybercrime, threats of terrorism, and so on. But there has been little consensus on how these aspects should be changed. Objections to proposed changes often cluster around several themes: excessively negative effects on privacy and civil liberties, ineffectiveness at achieving the stated goals of the proposed changes, excessive burdens placed on business, negative impact on innovation, to name a few of the most prominent.

7.8.2 International law[35]

International obligations arise from explicit treaties and customary international law (which are the customary practices of nations that are followed from a sense of legal obligation). Provisions of international law are sometimes the basis for national laws that are enforced by the domestic legal system. However, in the absence of national laws intended to satisfy treaty obligations or customary international law, the recourse mechanisms available for violation are far less robust than in domestic law. The International Court of Justice has held specific nations in violation of international law from time to time, but it lacks the ability to penalize nations for such violations. In principle, the U.N. Security Council can call for coercive military action that forces a violator to comply with its resolutions, but such options are not always viable in practice.

Aspects of international law relevant to cyber policy and security include the laws of armed conflict, human rights law, trade law, and various bilateral arrangements (e.g., mutual legal assistance treaties). The United States has authoritatively stated its view that the principles of international law apply to cyberspace.[36] In June 2013, a Group of Governmental Experts tasked by the United Nations noted that "International law, and in particular the Charter of the United Nations, is applicable and is essential to maintaining peace and stability and promoting an open, secure, peaceful and accessible ICT [information and communications technology]

[35] The discussion of this section owes much to Chapter 7 of the NRC report, Owens, Dam and Lin, *Technology, Policy, Law, and Ethics Regarding U.S. Acquisition and Use of Cyberattack Capabilities*, NAP, Wash DC 2009.

[36] *International Law in Cyberspace*, remarks of Harold Hongju Koh, Legal Advisor of the U.S. Department of State, to the USCYBERCOM Inter-Agency Legal Conference, Ft. Meade, MD, September 18, 2012. Available at http://www.state.gov/s/l/releases/remarks/197924.htm.

environment."[37] Among the nations represented in this group were the United States, China, and Russia. The United States hailed this report as a major step forward,[38] even though it only made recommendations and is not binding on any nation. More recent developments appear to indicate that at least China may be backing away from the view expressed in the report, since subsequent statements from China underscoring other statements made in the report do not reference this point.

The laws of armed conflict (LOAC)

LOAC addresses two separate questions. First, when is it legal for a nation to use force against another nation? The body of law relevant to this question is known as jus ad bellum, and is composed of the United Nations Charter, interpretations of the U.N. Charter, and some customary international law that has developed in connection with and sometimes prior to the U.N. Charter. Second, what are the rules that govern the behavior of combatants who are engaged in armed conflict? Known as jus in bello, this body of law is separate and distinct from jus ad bellum. *Jus in bello* is largely composed of the Hague Conferences of 1899 and 1907, the Geneva Conventions, and customary international law.

Two of the most important provisions of jus ad bellum are Article 2(4) of the U.N. Charter, which prohibits every nation from using "the threat or use of force against the territorial integrity or political independence of any state, or in any other manner inconsistent with the Purposes of the United Nations," and Article 51, which provides that "Nothing in the present Charter shall impair the inherent right of individual or collective self-defence if an armed attack occurs against a Member of the United Nations, until the Security Council has taken measures necessary to maintain international peace and security." Self-defense contemplated by Article 51 does not require Security Council authorization.

Jus in bello addresses issues related to military necessity (valid targets are only those whose damage or destruction would produce a military advantage); proportionality (collateral damage is allowable, but not if the foreseeable collateral damage is disproportionate compared to the military advantage likely to be gained from the attack); perfidy (falsely claiming to have protected status under LOAC, such as being a medical facility that is legally immune from targeting); distinction (refraining from deliberately attacking civilians or civilian assets)

How LOAC should be interpreted in the context of cyber conflict between nations is unresolved, though their importance is largely unquestioned. Such legal uncertainty arises because there is not a large body of actual experience in considering how these provisions might be relevant to cyber conflict, at least in part because the U.N. Charter and other foundational documents were written long before the advent of the information technology that enables cyber conflict.

[37] See http://www.un.org/ga/search/view_doc.asp?symbol=A/68/98.
[38] http://www.state.gov/r/pa/prs/ps/2013/06/210418.htm

One of the most authoritative though still unofficial attempts to bring clarity to the application of LOAC to cyber conflict is the Tallinn Manual on the International Law Applicable to Cyber Warfare.[39] This manual is the product of a multi-year project involving a number of international law scholars and practitioners and 95 "black-letter rules" governing such conflicts, addressing topics such as sovereignty, State responsibility, international humanitarian law, and the law of neutrality. Commentary accompanies each rule, which describes the rule's basis in treaty and customary law, explains how the group interpreted applicable norms in the cyber context, and outlines disagreements within the group as to each rule's application.

Human rights law

The major treaty relevant to human rights law is the International Covenant on Civil and Political Rights (ICCPR).[40] Two of the rights enumerated in the ICCPR may be relevant to the cyber domain in particular. Article 17 (protecting privacy and reputation) might speak to cyber activities intended to harm the reputation of an individual, e.g., by falsifying computer-based records about transactions in which he or she had engaged, or to uncover private information about an individual. Article 19 (protecting rights to seek information) might speak to cyber activities intended to prevent citizens from obtaining access to the Internet or other telecommunications media, although the Article 19 right is subject to certain restrictions for respecting of the rights or reputations of others; for protecting national security, public order, public health or morals and by Article 20, which prohibits propaganda for war and advocacy of national, racial or religious hatred that constitutes incitement to discrimination, hostility or violence.

Disagreements about the scope of Article 19 are at the heart of human rights concerns about Internet censorship and advocacy of the "free and open Internet" agenda. From a Western perspective, policies and technologies to advance this agenda and to weaken censorship in repressive nations take center stage. As one illustration, then-Secretary of State Hillary Clinton chastised a number of nations, including China, Tunisia, Uzbekistan, and Vietnam for Internet censorship.[41] A more recent development is the reported attempt by China to take aggressive action in cyberspace against parties that actively support the anti-censorship agenda. Dubbed the "Great Cannon" by the Munk Center,[42] a Chinese cyberattack tool has been used to manipulate the traffic of "bystander" systems outside China that happen to touch to cause these bystander systems to launch a distributed denial of service attack against sites that provide censorship circumvention tools and services.

Trade law

[39] Michael Schmitt et al, *Tallinn Manual on The International Law Applicable To Cyber Warfare*, Cambridge University Press, 2013. Available at http://www.cambridge.org/us/academic/subjects/law/humanitarian-law/tallinn-manual-international-law-applicable-cyber-warfare.

[40] http://www.ohchr.org/en/professionalinterest/pages/ccpr.aspx

[41] http://www.state.gov/secretary/20092013clinton/rm/2010/01/135519.htm

[42] https://citizenlab.org/2015/04/chinas-great-cannon/

The World Trade Organization (WTO) is an international organization addressing the rules of trade between nations.[43] A variety of agreements, such as the Agreement on Trade-Related Aspects of Intellectual Property Rights (TRIPS), were negotiated under the WTO's auspices. The TRIPS agreement describes how basic principles of the trading system and other international intellectual property agreements should be applied; how to give adequate protection to intellectual property rights; how countries should enforce those rights adequately in their own territories; how to settle disputes on intellectual property between members of the WTO; and special transitional arrangements during the period when the new system is being introduced.

Given that a major international issue in cyberspace relates to the theft of intellectual property and cyber-enabled economic espionage, some analysts have suggested that the United States and other nations should file a proceeding against China in the WTO for unfair trade practices, i.e., for intellectual-property theft or infringement that may undermine stable, competitive global trade.[44] According to this logic, a WTO ruling against China would "provide a strong basis for the United and other aggrieved nations to lawfully impose tough economic sanctions that China would find highly undesirable."

Countermeasures and unfriendly acts

International law also recognizes the concept of countermeasures.[45] According to Schmitt,[46] countermeasures are "State actions, or omissions, directed at another State that would otherwise violate an obligation owed to that State and that are conducted by the former in order to compel or convince the latter to desist in its own internationally wrongful acts or omissions." That is, countermeasures taken by B against A would themselves be unlawful actions were it not for the wrongful actions of A against B. B's countermeasures must be taken only for the purpose of persuading A to desist in A's wrongful actions. Moreover, countermeasures are relevant only when A's wrongful actions do not rise to the threshold of a "use of force" or "an armed attack" as the latter terms are defined in the UN Charter. (If A's actions do rise to these levels, Article 2(4) and Article 51 of the UN Charter come into play.)

Countermeasures are subject to two constraints. First, they must themselves be below the threshold of a use of force or an armed attack. Second, the provoking action must in fact be

[43] https://www.wto.org/english/thewto_e/whatis_e/tif_e/agrm7_e.htm

[44] James P. Farwell, "Take Chinese Hacking to the WTO", National Journal, March 15, 2013 http://nationalinterest.org/commentary/take-chinese-hacking-the-wto-8224

[45] In this context, the term "countermeasures" is a legal term that contrasts with its more technical usage. For cyber weapons, technical countermeasures might refer to the use of antivirus scanners to detect computer viruses or active defense measures using cyber weapons to inflict damage or pain against a cyber intruder. This technical usage is NOT applicable to this section.

[46] Michael Schmitt, "'Below the Threshold' Cyber Operations: The Countermeasures Response Option and International Law", 54 Virginia Journal of International Law __ (2014), http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2353898.

attributable to a specific responsible nation (in the example above, A must be known to be a specific nation that is in fact responsible for the action).

Unfriendly acts are yet another category of possible response to cyber intrusions. According to the Oxford Public International Law Encyclopedia,[47] an “unfriendly act” is conduct (act or a failure to act)) that “inflicts a disadvantage, disregard or discourtesy on another subject of international law without violating any legal norm.” A State acting in an unfriendly manner towards another must have a reason for such action, but in principle any perceived effrontery can suffice.

Codes of Conduct

Codes of conduct seek to define standards and principles that guide the behavior of parties accepting those codes. Codes of conduct are not in and of themselves legally binding, although a particular code of conduct that is voluntarily agreed to by a large number of nations is well on its way to being established as customary international law. Of particular note is a joint presentation in September 2011 by China, Russia, Tajikistan and Uzbekistan supporting a possible UN General Assembly resolution on an international code of conduct for information security.[48] The purpose of this code would be to “ensure that information and communications technologies, including networks, are to be solely used to benefit social and economic development and people’s well-being, with the objective of maintaining international stability and security.” In particular, this code called for signatories “not to use information and communications technologies, including networks, to carry out hostile activities or acts of aggression, pose threats to international peace and security or proliferate information weapons or related technologies.”

Bilateral and multilateral arrangements

Nations around the world enter into bilateral and multilateral treaties and other arrangements. For example, the Budapest convention is an international agreement among several dozen nations (mostly but not entirely in the liberal western democracies) to, among other things, enact domestic laws that criminalize certain kinds of behavior in cyberspace.[49] (That is, it can be regarded as an agreement to harmonize these laws across national boundaries.) Some of the behaviors in question include illegal access to a computer, illegal interception of data, data interference, system interference, misuse of devices, and the use of a cyber weapon could be included under these rubrics. In addition, the convention seeks to enhance the effectiveness of transnational law enforcement activities against cyber crime. Nations may also pledge to behave towards each other in particular ways—on May 8, 2015, the Wall Street Journal reported that China and Russia have agreed not to conduct cyber attacks against each other, and to jointly counteract technology that may “destabilize the internal political and socio-

[47] http://opil.ouplaw.com/view/10.1093/law:epil/9780199231690/law-9780199231690-e423
[48] http://daccess-dds-ny.un.org/doc/UNDOC/GEN/N11/496/56/PDF/N1149656.pdf
[49] http://conventions.coe.int/Treaty/en/Treaties/Html/185.htm

economic atmosphere," "disturb public order" or "interfere with the internal affairs of the state."[50]

7.8.3 Some interesting questions in the legal domain for cyber policy and security

Given the broad purview of domestic and international law, any finite set of interesting questions relevant to cyber policy and security is necessarily restrictive and arbitrarily truncated. That said, here are a few questions that I find interesting.

- In April 2015, the White House issued an executive order allowing the imposition of economic sanctions against parties overseas who engage in certain harmful cyber activities against the United States. Such sanctions may include freezing their financial assets, barring U.S. commercial transactions with them, and barring them from traveling to the United States.[51] Use of such economic sanctions does not rise to the level of armed attack or a use of force and is thus one step in expanding the range of options that the United States has for responding to hostile cyber activities. However, what is less clear is how targets of such sanctions—and the nations of which these targets are associated—will respond themselves if such sanctions are imposed. For example, it is easy to imagine that the nations might respond to U.S. action by increasing the burdens on U.S. companies doing business with them. Understanding how the imposition of these sanctions is likely to play out over many moves, not just one, is an important aspect of starting down this path in the first place.[52]

- As noted above, China, Russia, Tajikistan and Uzbekistan proposed an international code of conduct for information security in September 2011. The U.S. response to this proposal was to oppose it. Although the United States had good reason to oppose the proposed code, it did not table an alternative code of conduct. As a political matter, the absence of an alternative U.S. proposal may have left the United States at a disadvantage. If so, it is interesting to consider what principles and guidelines should be included in an alternative code of conduct that the United States could endorse.

- The current legal regime governing electronic surveillance in the United States is ill-suited to the technological realities of today. For example, one website of reform advocates argues that the current regime is "a patchwork of confusing standards that have been interpreted inconsistently by the courts, creating uncertainty for both service providers and law enforcement agencies.[53] In 2002, the Ninth Circuit Court of Appeals

[50] http://blogs.wsj.com/digits/2015/05/08/russia-china-pledge-to-not-hack-each-other/

[51] http://www.nytimes.com/2015/04/02/us/politics/us-expands-foreign-cyberattack-retaliation-options.html?_r=0 . The text of the order itself can be found at https://www.whitehouse.gov/the-press-office/2015/04/01/executive-order-blocking-property-certain-persons-engaging-significant-m.

[52] http://www.lawfareblog.com/2015/04/a-worry-about-the-new-executive-order-on-sanctions-for-malicious-cyber-activity/

[53] http://digitaldueprocess.org/index.cfm

wrote that the intersection of these two statutes [the Wiretap Act and the Stored Communications Act, both included in the ECPA regime] "is a complex, often convoluted, area of the law. . . . The existing statutory framework [that is, the ECPA regime] is ill-suited to address modern forms of communication. . . Courts have struggled to analyze problems involving modern technology within the confines of this statutory framework, often with unsatisfying results. We observe that until Congress brings the laws in line with modern technology, protection of the Internet and websites . . . will remain a confusing and uncertain area of the law."[54] Even the Department of Justice noted in April 2011 that portions of ECPA [i.e., the current legal regime] "may be appropriate for further legislation or clarification."[55] In light of technological changes since the original inception of the current regime, what should be the content of a new regime that is better suited to deal with the present and reasonably anticipated future technological reality?

- As discussed in Section 7.3, the private sector is apparently forbidden to undertake offensive actions to protect their interests in cyberspace. The Computer Fraud and Abuse Act is one important bar to such action, and the Economic Espionage Act may be another. But a self-defense justification for an admitted violation of the Computer Fraud and Abuse Act has never been attempted in court, and thus it is an interesting question as to the circumstances, if any, that would enable such a defense would succeed. A related question is how the Act could be modified, if at all, in such a way as to allow certain offensive actions to be taken in such defense in a "sensible" way, whatever that term might mean.

7.9 Ethical implications of cyber policy and security

Cyber policy and security have many ethical implications. Because law is arguably intended to reflect considered ethical judgments, one obvious set of ethical implications arises out of legal considerations that may impinge on any given policy position. Also, in practice, one finds that nearly every decision meant to improve cyber policy or security potentially raises concerns about privacy or civil liberties. In any given instance, such concerns may (or may not) be easy to address, but what is not right is to dismiss them out of hand.

Several other issues that raise ethical concerns are described below.

- Hacktivism can be defined as the use of computers and computer networks as a means of protest to promote political or social ends that does not rise to the level of severely harming civilians. Hacktivism uses offensive cyber operations to promote ends that at least some people regard as entirely ethical. For example: Is it ethical for a group of hackers to take down a website that is being used primarily to trade child pornography,

[54] 302 F.3d 868, 886 (9th Cir. 2002) , available at https://law.lclark.edu/live/files/7301-konoppdf.
[55] http://fas.org/irp/congress/2011_hr/ecpa.pdf

traffic in stolen credit card numbers, or support terrorist operations? Is it ethical for hacktivists protest the policies or practices of governments or corporations by defacing websites or conducting web “sit-ins?”[56]

- In her Internet freedom speech (Footnote 41), Secretary of State Clinton also called attention to the need for more secure information systems and networks around the world, noting that the United States has “taken steps as a government, and as a Department [i.e., the Department of State], to find diplomatic solutions to strengthen global cyber security.” However, the United States has also been increasingly open about its interests in conducting offensive operations in cyberspace—conduct that requires cyberspace targets to be as insecure as possible. Furthermore, with the Snowden disclosures about U.S. offensive capabilities still in the world’s consciousness, the tension between these two goals is obvious—and other nations have openly called the United States hypocritical. On the other hand, Farrell and Finnemore write about hypocrisy as a strategic resource,[57] a point that leads to an obvious question—why should nations be expected to behave consistently when they have to balance multiple interests? How and to what extent, if any, is the hypocrisy of the United States ethically questionable?

- Some individuals who break into computer systems without authorization (in violation of the Computer Fraud and Abuse Act and contrary to the wishes of the owners and operators of those systems) claim that they are performing a public service by demonstrating the insecurity of these systems. For example, defense lawyers for the person responsible for the first widespread Internet virus—Robert Morris—made just such an argument.[58] How and to what extent, if at all, do such claims withstand ethical scrutiny?

- A government that discovers or otherwise comes into possession of a zero-day vulnerability may keep it for future use in some adversarial or offensive cyber operation conducted for national purposes or fix/report it to reduce the susceptibility to penetration of the systems in which that vulnerability is found. In a blog post in April 2014, Michael Daniel, Special Assistant to the President and the White House Cybersecurity Coordinator, wrote about these choices from the perspective of the U.S.

[56] http://faculty.nps.edu/dedennin/publications/Ethics%20of%20Cyber%20Conflict.pdf

[57] Henry Farrell and Martha Finnemore, “The End of Hypocrisy: American Foreign Policy in the Age of Leaks”, *Foreign Affairs*, November/December 2013. Available at https://www.foreignaffairs.com/articles/united-states/2013-10-15/end-hypocrisy.

[58] Bryan Smith, William Yurcik, and David Doss, “Ethical Hacking: The Security Justification,” *Proceedings of the Ethics of Electronic Information in the 21st Century Symposium (EEI21)*, University of Memphis, Memphis TN USA, October 18-21 2001. http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.24.1733&rep=rep1&type=pdf.

government.[59] He said that "building up a huge stockpile of undisclosed vulnerabilities while leaving the Internet vulnerable and the American people unprotected would not be in our national security interest. But that is not the same as arguing that we should completely forgo this tool as a way to conduct intelligence collection, and better protect our country in the long-run. Weighing these tradeoffs is not easy... " What are the ethical implications of the keep/disclose choice?

8. Conclusion

In the mid-1980's, Paul Doty—the founder of the Kennedy School's Center for Science and International Affairs at Harvard University (now the Belfer Center) and a pioneer in the field of science and international affairs as applied to problems of international security—had a ready answer to any student who came to him in search of an interesting problem. He would hand the student a short document on which were printed some two or three dozen problems in arms control and international security. Each problem was described in a paragraph and had a question attached to it. Some problems were scaled to be PhD theses, others undergraduate term papers, and many others fell in between these extremes.

This paper has only scratched the surface of interesting problems in cyber policy and security. Over time, I hope that this document will itself evolve into to include a list of interesting problems for cyber policy and security, in just the same way that the Doty list did (though future iterations of this document will be on the Web). I invite any and all to propose their candidate problems—the question, an explanatory paragraph, and a scaling of the size of the problem. If included on this future list, full credit for submission will be provided.

[59] https://www.whitehouse.gov/blog/2014/04/28/heartbleed-understanding-when-we-disclose-cyber-vulnerabilities

Appendix A

A Brief Primer on the Tools and Techniques of Cyber Conflict[60]

In the 21st century, information is the key coin of the realm, and thus entities from nation-states to individuals are increasingly dependent on information and information technology (to include both computer and communications technologies). Businesses rely on information technology (IT) to conduct operations (e.g., payroll and accounting, recording inventory and sales, research and development (R&D). Distribution networks for food, water, and energy rely in IT at every stage, as do transportation, health care, and financial services. Factories use computer-controlled machinery to manufacture products more rapidly and more efficiently than ever before.

Military forces are no exception. IT is used to manage military forces (e.g., for command and control and for logistics). The use of IT embedded in modern weapons systems increases the lethality and reduces the collateral damage associated with the use of such weapons. Movements and actions of military forces can be coordinated through networks that allow information and common pictures of the battlefield to be shared widely.

Given the increasing importance of information and IT throughout all aspects of modern life and society, it is not surprising that different actors in cyberspace might seek to gain advantage over others by using various tools and techniques for taking non-consensual advantage of certain aspects of cyberspace—what this paper will call “conflict in cyberspace” or “cyber conflict.” This definition implies that “armed conflict” or “military conflict” are subsets—and only subsets—of the broader term “conflict,” which may entail a conflict over economic, cultural, diplomatic, and other interests as well as conflict involving military matters or the use of arms. This means, for example, that consumers concerned about protecting their privacy and governments seeking to obtain their personal data may be engaged in a form of cyber conflict.

This primer on the tools and techniques of cyber conflict is very short, basic, and not comprehensive; knowledgeable readers may wish to skip this section.

The tools and techniques of conflict in cyberspace can be usefully separated into tools based on technology and techniques that focus on the human being. Offensive tools and techniques allow a hostile party to do something undesirable. Defensive tools and techniques seek to prevent a hostile party from doing so.

[60] Much of the material in this primer is adapted from National Research Council, *At the Nexus of Cybersecurity and Public Policy: Some Basic Concepts and Issues,* David Clark, Thomas Berson, and Herbert Lin (eds.), National Academies Press, Washington D.C., 2014; Herbert Lin, *Cyber Conflict and National Security*, in *International Politics: Enduring Concepts and Contemporary Issues*, Robert Art and Robert Jervis (eds.); and Herbert Lin, “Cyber Conflict and International Humanitarian Law,” *International Review of the Red Cross*, 94(886):515-531, Summer 2012, available at https://www.icrc.org/eng/resources/documents/article/review-2012/irrc-886-lin.htm.

Technology-based tools

An offensive tool requires three components:

- Access refers to how the hostile party gets at the IT of interest. Access may be remote (e.g., through the Internet, through a dial-up modem attached to it, through penetration of the wireless network to which it is connected). Alternatively, access may require close physical proximity (e.g., spies acting or serving as operators, service technicians, or vendors). Close access is a possibility anywhere in the supply chain (e.g., during chip fabrication, assembly, loading of system software, during shipping to the customer, during operation).

- A vulnerability is an aspect of the IT that can be used to compromise it. Vulnerabilities may be accidentally introduced through a design or implementation flaw, or introduced intentionally (see close-access above). An unintentionally introduced defect ("bug") may open the door for opportunistic use of the vulnerability by an adversary.

- Payload is the term used to describe the mechanism for affecting the IT after access has been used to take advantage of a vulnerability. For example, once a software agent (such as a virus) has entered a computer, its payload can be programmed to do many things—reproducing and retransmitting itself, destroying files on the system, altering files. Payloads can be designed to do more than one thing, or to act at different times. If a communications channel is available, payloads can be remotely updated.

Defensive tools address one or more of these elements. For example, some tools (e.g., firewalls) close off routes of access that might be inadvertently left open. Other tools identify programming errors (vulnerabilities) that can be fixed before a hostile party can use them. Still others serve to prevent a hostile party from doing bad things with any given payload (e.g., a confidential file may be encrypted so that even if a copy is removed from the system, it is useless to the hostile party).

People-based techniques

People interact with information technology, and it is often easier to trick, bribe, or blackmail an insider into doing the bidding of a hostile party. For example, close access to a system may be obtained by bribing a janitor to insert a USB flash drive into a computer. A vulnerability may be installed by blackmailing a programmer into writing defective code. Note that in such cases, technical tools and people-based techniques can be combined.

Defensive people-based techniques essentially involve inducing people to not behave in ways that compromise security. Education teaches (some) people not to fall for scams that are intended to obtain log-in names and passwords. Audits of activity persuade (some) people not to use IT in ways that are suspicious. Rewards for reporting persuade (some) people to report questionable or suspicious activity to the proper authorities.

The nature of offensive activity in cyberspace

Offensive activity in cyberspace can be described as cyberattack or cyber exploitation.

- Cyberattack refers to the use of deliberate activities to alter, disrupt, deceive, degrade, or destroy computer systems or networks used by an adversary or the information and/or programs resident in or transiting these systems or networks. The activities may also affect entities connected to these systems and networks. A cyberattack might be conducted to prevent authorized users from accessing a computer or information service (a denial of service attack), to destroy computer controlled machinery (the alleged purpose of the Stuxnet cyberattack[61]), or to destroy or alter critical data (e.g., timetables for the deployment of military logistics). Note that the direct effects of a cyberattack (damage to a computer) may be less significant than the indirect effects (damage to a system connected to the computer).

- Cyber exploitation refers to deliberate activities to penetrate computer systems or networks used by an adversary for obtaining information resident on or transiting through these systems or networks. Cyberexploitations do not seek to disturb the normal functioning of a computer system or network from the user's point of view—indeed, the best cyberexploitation is one that such a user never notices. The information sought is generally information that the adversary wishes not to be disclosed. A nation might conduct cyber exploitations to gather for valuable intelligence information, just as it might deploy human spies to do so. It might seek information on an adversary's R&D program for producing nuclear weapons, or on the adversary's order of battle, its military operational plans, and so on. Or it might seek information from a company's network in another country in order to benefit a domestic competitor of that company. A private company could seek the click streams of a user to identify his or her interests as a consumer.

Note that press accounts often refer to cyberattacks when the activity conducted is a cyber exploitation.

Cyberattacks and cyber exploitations can be regarded as offensive operations. Offensive operations in cyberspace use offensive tools as described above, but just as a military operation involves much more than a bunch of people shooting their guns, an offensive operation in cyberspace involves tactics, procedures, scheduling and sequencing of various activities, intelligence gathering, assessment, and so on. For example, an offensive operation may conduct an exploitations that will additional information to make an later exploitation or attack more effective. Perhaps most importantly, offensive operations are conducted by people with goals in mind.

[61] A primer on Stuxnet can be found at http://topics.nytimes.com/top/reference/timestopics/subjects/c/computer_malware/stuxnet/index.html?scp=1-spot&sq=stuxnet&st=cse.

Who might conduct offensive operations in cyberspace? The nature of information technology is such that the range of actors who can conduct operations of national-level significance is potentially large. Certain nation states, such as the United States, China, Russia, and Israel, are widely regarded as having potent offensive cyber capabilities, although smaller nation states can also conduct offensive operations in cyberspace.

A variety of subnational actors—including individuals, organized crime, and terrorists—might conduct cyberattacks and/or cyber exploitations. Indeed, some (but only some) such operations can be conducted with information and software found on the Internet and hardware easily available by mail order.

Motivations for conducting such operations also span a wide range. One of the most common reasons today is financial. Because a great deal of commerce is enabled through the Internet or using IT, some parties are cyber criminals who seek illicit financial gain through their offensive actions. Cyber exploitations can yield valuable information, such as credit card numbers or bank log-in credentials; trade secrets; business development plans; or contract negotiation strategies. Cyberattacks can disrupt the production schedules of competitors, destroy valuable data belonging to a competitor, or used as a tool to extort money from a victim. Perpetrators might conduct a cyberattack for hire (it is widely believed that the cyberattack on Estonia was conducted using a rented cyber weapon).

The commercial dimension is important as well. Much of electronic commerce is based on taking advantage of information about consumers, and those who collecting such information may obtain it in ways and in volumes that are not entirely apparent to consumers.

Another possible reason for such operations is political—the perpetrator might conduct the operation to advance some political purpose. A cyberattack or exploitation may be conducted to send a political message to a nation, to gather intelligence for national purposes, to persuade or influence another party to behave in a certain manner, or to dissuade another party from taking certain actions.

Still another reason for conducting such operations is personal—the perpetrator might conduct the operation to obtain “bragging rights,” to demonstrate mastery of certain technical skills, or to satisfy personal curiosities.

Lastly, such operations may be conducted for military reasons, in the same way that traditional military operations involving kinetic weapons are used.

<u>The nature of defensive activity in cyberspace</u>

Broadly speaking, there are a limited number of approaches to defend against offensive cyber threats. As described below, these approaches are not mutually exclusive.

- Reducing reliance on information technology. For example, a classic way to reduce such reliance is to eliminate or block known but unnecessary access paths. Many IT systems or networks have a variety of ways to access them that are unnecessary for their effective use. For example, unneeded wireless connections and wired jacks may be disabled. Disconnecting from the Internet is a well-known way to eliminate an access path (but obviously such disconnection does not eliminate ALL possible access paths). One might also consider whether automation in any given instance actually provides benefits that are worth the costs in security as well as in other ways.

- Reducing the number of vulnerabilities contained in any deployed IT system or network, by fixing vulnerabilities as soon as they become known and/or by designing and implementing software so that it has fewer vulnerabilities from the start. In some cases, hardware-based security features are feasible—implementing such features in hardware is often more secure than implementing them in software, although they may be less flexible than comparable software implementations.

- Making better and more effective the use of known security technologies and practices. Many technologies and practices that would strengthen security are not used because they are inconvenient, expensive, or both and hence get in the way of doing useful work. Appropriate incentives can promote the use of known security technologies and practices and help to remove barriers that impede their use.

- Working through adversary compromise. Even the best defenses will not keep intruders at bay forever. Users of information technology systems and networks should be able to work through the problems caused by a compromised system, although quite possibly at the cost of reduced functionality and/or efficiency. An adversary who successfully penetrates a system or network should not thereby obtain free rein to do anything inside the system—the impact of such a penetration should be contained. Damage done by an adversary should be reversible—this is the intent of recovery. (A simple example is that file backups can be used to restore data lost during an attack.) And resilience implies that compromising one function or part of a large system or network does not render everything unusable.

- Reducing the threat posed by adversaries. One approach to reducing the threat is deterrence—threats of punishment against an adversary for misbehavior are intended to persuade the adversary not to engage in that misbehavior, and such an adversary, so deterred, does not engage in efforts that will compromise the systems or networks in question. Another approach to threat reduction is based on agreements with adversaries to behave or not to behave in certain ways so as to reduce the threat that each side poses to the other—when such agreements are honored, compromising behavior is less likely to occur and the systems or networks in question are more safe. Still another approach to threat reduction is active defense, in which the side under threat takes offensive action itself against adversaries to reduce their threatening capabilities.

A critical point about this array of possibilities is that technical defenses do not suffice. In general, such defenses are deployed against specific technical threats rather than specific adversaries; as defenses are erected, adversaries will find other means to attack. Furthermore, such defenses are invariably imperfect: They can reduce threats but cannot eliminate them entirely. To be useful, computer systems need programs and data supplied externally. Of course, only if the programs and data are "good"—that is, they are what the user wants them to be—will these systems produce results that are good. However, there is no general method for assuring that the programs and data supplied to the computer are in fact "good".

The offense-defense relationship

Offense and defense have a complex relationship in cyberspace. If the adversary does not care about when his efforts are successful, the adversary has an enormous advantage. The reason is that under these circumstances, defensive measures must succeed every time an adversary conducts a hostile action, and the adversary's action need succeed only once. These facts place a heavy and asymmetric burden on the defender.

The overwhelming advantage of the offense changes, sometimes dramatically, if the adversary must operate under time constraints. Under these circumstances, the adversary does not have an infinite number of tries. Technical success in penetrating the system may eventually occur, but it may happen too late for that penetration to be useful.

Appendix B

Worked Example #1: Escalation Dynamics and Conflict Termination in Cyberspace

In recent years, planning for U.S. national security has contemplated the possibility that the United States would deter or might be engaged in conflict of various kinds in cyberspace. Should deterrence fail, such engagement could entail the United States as the target of hostile cyber operations, as the initiator of cyber operations against adversaries, or some combination of the two.

Much of the serious analytical work related to cyber conflict to date focuses on the initial transition from a pre-conflict environment to an environment in which cyber conflict is known to be taking place. Indeed, studies on deterrence of cyber conflict focus primarily on how to make the initial transition as unlikely or difficult as possible.

Little work has been done on three key issues: how the initial stages of conflict in cyberspace might evolve or escalate (and what might be done to prevent or deter such escalation); how cyber conflict at any given level might be de-escalated or terminated (and what might be done to facilitate de-escalation or termination); and how cyber conflict might escalate into kinetic conflict (and what might be done to prevent kinetic escalation). Each of these issues is important to policy makers, both in managing a crisis and in preparing for it.

The phenomenon of escalation in conflict is a change in the level of conflict (defined in terms of scope, intensity, or both) from a lower (perhaps non-existent) level to a higher level. Escalation is a fundamentally interactive concept, in which actions by one party trigger other actions by another party to the conflict. Of particular concern is a chain reaction in which these actions feed off of one another, thus raising the level of conflict to a level not initially contemplated by any party to the conflict.

Theories of escalation dynamics have been most elaborated in the nuclear domain. But the deep and profound differences between the nuclear and cyber domains suggest that any theory of escalation dynamics in the cyber domain would require far more than small perturbations in theories of nuclear escalation dynamics, though such theories might be useful points of departure for the development of new theory applicable to cyberspace. Some of these differences include the greater uncertainties in attribution of cyber actors; the broad proliferation of significant capabilities for cyber operations to a multitude of states and to a variety of nonstate actors as well; and the inherent ambiguities of cyber operations as compared to the very distinct threshold of nuclear weapons explosions.

As an example of an ambiguous cyber operation, consider the difference between two types of cyber activities: espionage and attack. The general form of a cyber intrusion involves a penetration to the inside of a computer system or network and a payload that executes to perform some hostile function. Such a function may be destructive or damaging (a cyberattack that alters or destroys information on the targeted system), or it may be exfiltrative (a cyber exploitation that clandestinely removes information from the targeted system). Although the intruder may know the intent underlying the intrusion, the victim may well see only the penetration and may not know the purpose (attack or exploitation?) until the payload executes. Such confusion on the victim's part may cause him to misinterpret the intrusion—he may see an attack when the intruder intended only an exploitation, or vice versa—and thus to react inappropriately. An inappropriate response may well be dangerous to both sides.

Conflict termination presumes the existence of an ongoing conflict to which the participants desire an end. Conflict termination requires several elements:

- A reliable and trustworthy mechanism that can be used by the involved parties to negotiate the terms of an agreement to terminate a conflict.
- A clear understanding on all sides about what the terms of any agreement require each side to do.
- Assurance that all parties to an agreement will adhere to the terms of any such agreement.
- Capabilities for each party that can insure that all entities taking action on behalf of that party adhere to the terms of any such agreement.
- Reliable electronic channels on which national leaders can communicating in the midst of certain kinds of cyber conflict.

Issues of escalation and conflict termination in cyberspace are complicated by the fact that there may be cross-domain linkages. Although conflict might, in principle, be limited to hostile operations in cyberspace alone, there is no reason that this is necessarily so, and policy makers must contemplate the possibility that conflict in cyberspace might spill over into physical space, and might even lead to kinetic actions.

U.S. military doctrine for taking advantage of cyberspace seems to emphasize the utility of early use, that is, early in a conflict that will eventually entail kinetic operations. In addition, the logic of offensive cyber operations suggests that such operations are likely to be most successful when the initiator of these operations has the time to gather intelligence on likely targets—such intelligence-gathering is obviously time-limited once overt conflict does break out.

On the other hand, the use of kinetic operations during an ostensibly cyber-only conflict is an important threshold. Nations involved in a cyber-only conflict may have an interest in refraining from a kinetic response—for example, they may believe that kinetic operations would be too provocative and might result in an undesired escalation of the conflict.

If understanding the dynamics of cyber-only conflict is difficult, understanding the dynamics of cyber conflict when kinetic operations may be involved is doubly so.

Against this backdrop, some of the key research questions regarding escalation dynamics in cyberspace include the following:

- How and to what extent can the parties to a negotiation share an understanding of key concepts (e.g., what constitutes an “attack” in cyberspace)? How can differences in understanding best be resolved?
- How can one party know that the other party has ceased hostile activity in cyberspace, given difficulties in attribution, in distinguishing between cyber operations for attack and exploitation, and in the lack of national technical means that can verify a stand-down of cyber forces?
- How can a nation manage its own “patriotic hackers”, who might otherwise cause an adversary to misperceive their national government’s intent?
- What thresholds of unacceptable activity might be created in cyberspace and how might these be communicated to an adversary?
- How might the United States deter escalation when it arguably has more at stake in cyberspace than its adversaries?
- What means are available to signal intent to adversaries in cyberspace, and how might these means be used?
- How and to what extent, if any, does the body of empirical evidence about cyber intrusions perpetrated by nation states (or non-state actors, for that matter) speak to escalation dynamics in cyber conflict? Which aspects of such experience, if any, give insights into applicability or relevance of analogies or theories from other realms?
- How might nations reassure each other about their intentions in cyberspace, especially during times of tension or conflict? What, if any, is the role of confidence-building measures? What steps can feasibly be taken to improve transparency in cyberspace that will improve the prospects for managing cyber conflict successfully?
- How can national authorities exercise effective command and control of cyber forces in a rapidly evolving unfolding conflict environment? (Cyber forces necessarily include software-based or hardware-based agents that may be operating autonomously or semi-autonomously. Note also that during conflict, various communications paths used prior to conflict may be compromised or unavailable.)
- What is the scope and nature of national capabilities (e.g., technological, command-and-control, law enforcement/legal capabilities) needed to implement any approach to escalation management and conflict termination in cyberspace? How can each side obtain realistic assessments of an adversary’s cyber state and condition (e.g., heavily or damaged)?
- How might other resources/capabilities available to a nation such as the United States be used manage escalation of conflict in cyberspace?
- What does “victory” mean in a cyber conflict? What measures should be used to indicate when victory has been achieved?
- How and to what extent, if any, do force employment concepts such as counterforce and countervalue targeting remain useful in a cyber context for thinking about escalation dynamics?
- How might cyber conflict result in kinetic conflict? What might be done to forestall such escalation? How and to what extent, if any, do theories about escalation from

conventional to nuclear warfare provide guidance in exploring the cyber-to-kinetic transition?

- What is the significance with respect to escalation of cyber attack capabilities to neutralize adversary weaponry, whether conventional or nuclear, taking into account the uncertainties of damage assessment inherent in any offensive cyber operation?

Each of these questions is a research project in itself, and can be addressed usefully at a number of levels of effort, from term paper to doctoral thesis. In some cases, the question might be the basis for the conduct of a table-top exercise or war game whose unfolding would be the focus of research.

Appendix C

Legal and Policy Issues in Active Cyber Defense

The limitations of passive defenses to protect important information technology assets and the information they contain are well-known. Passive defenses, which may include (for example), repair of system vulnerabilities that enable an adversary's attack, updates of its anti-malware detection and removal software, and the shut-off of non-essential services that may be granting an adversary improper access are limited to IT assets within an organization's span of control—that is, systems and networks that it has the legal right to access, monitor, and modify. Furthermore, tightening security through the use of passive defenses often reduces important functionality in the systems being locked down—they become more difficult, slower, and inconvenient to use. Lastly, such measures are unlikely by themselves to be effective in the long run, because sustaining a locked-down posture is costly and believed by many to be insufficient in the face of a determined, well-resourced attacker who can make multiple attempts to breach defenses.

Recognizing the limitations of locking down systems and networks as the only option for responding to the cyber threat, the U.S. Department of Defense established Cyber Command, whose mission statement states that Cyber Command will conduct "activities to operate and defend the Department of Defense information networks and when directed, conducts full-spectrum military cyberspace operations (in accordance with all applicable laws and regulations) in order to ensure U.S. and allied freedom of action in cyberspace…."[62] In 2011, the U.S. Department of Defense issued its Strategy for Operating in Cyberspace (SOC), which states that the U.S. will employ "an active cyber defense capability to prevent intrusions onto DoD networks and systems." Taken together, the Cyber Command mission statement and the SOC emphasize the need for defense of U.S. military networks and systems against adversary threats, with full-spectrum military cyberspace operations to be conducted when directed to assist in that defense.

What is "active cyber defense"? The official DOD definition is that it is "DoD's synchronized, real-time capability to discover, detect, analyze, and mitigate threats and vulnerabilities. It builds on traditional approaches of defending DoD networks and systems, supplementing best practices with new operating concepts. It operates at network speed using sensors, software, and intelligence to detect and stop malicious activity before it can affect DoD networks and systems. As intrusions may not always be stopped at the network boundary, DoD will continue to operate and improve upon its advanced sensors to detect, discover, map, and mitigate malicious activity on DoD networks."[63]

[62] http://www.stratcom.mil/factsheets/cyber_command/

[63] www.defense.gov/news/d20110714cyber.pdf

The DOD strategy for operating in cyberspace does not describe active cyber defense in any detail, but the formulation above for "active cyber defense" could, if read broadly, include any action outside the DOD's organizational span of control, any non-cooperative measure affecting or harming an attacker's IT systems and networks, any proactive measure, or any retaliatory measure, as long as such action was taken for the purpose of defending DOD systems or networks from that attacker. Some of the actions that could in principle be included under the rubric of active cyber defense are actions taken within and outside of the DOD's span of control.

In the category of actions taken within of the DOD's span of control are actions such as

- tracking and monitoring the actions of an intruder
- deception of an intruder (e.g., files with tempting but useless misinformation)
- rerouting and/or dropping traffic from an intruder
- slowing computer system responses to an intruder
- collecting forensic information on an intruder
- allowing interactions for DOD IT systems and networks only with whitelisted parties/software/computers
- reconfiguring DOD defenses and networks in real-time during an attack.

In the category of actions taken outside the DOD's span of control are actions such as

- inspecting and/or deleting packet in flight beyond DOD boundaries
- gathering intelligence on attacker IT systems through trace-back and hack-back
- remotely disable stolen software or documents
- disrupting attacking computers to neutralizing/weaken incoming threat
- preempting adversary attack capabilities

In addition, active defense (vs. active cyber defense) need not necessarily involve a cyber response, but in principle could be any action taken against any of an adversary's interests.

The most controversial actions under the rubric of active defense are those that are both intrusive and damaging. An intrusive action is one that is conducted against an adversary IT asset (and not against a friendly or neutral IT asset); a damaging action is one that reduces the functionality of that asset (e.g., it may disrupt the adversary's control over the asset). Some of the relevant issues include the nature of and confidence in identification of the adversary and asset, the nature of the damage to be caused, and the time scale on which the action must be taken (before, during, or after the attack).

If active cyber defense measures are an effective deterrent against cyber threats, they might significantly improve the overall national security posture of the U.S., which currently suffers from a spectrum of national-security-related cyber probing, espionage, and other cyber attacks. On the other hand, an active cyber defense could fuel an arms race in cyberspace, inflame international relations, or even trigger hostile cyber responses. That is, active cyber defense could be a stabilizing or destabilizing approach, and understanding the full range of possibilities and repercussions is important.

There are many legal and policy issues associated with active cyber defense. These include:

- How and to what extent, if at all, is effective damage limitation possible in cyberspace?
- To what extent, if at all, is delayed retaliation effective at dissuading adversaries from further attacks?
- What is the appropriate threshold for mounting what kinds of active cyber defense?
- What is the nature of the appropriate command and control arrangements for active cyber defense? (For example, how and to what extent can and should rules of engagement be pre-programmed for automated responses?)
- How and to what extent, if any, does active cyber defense require cooperation with other actors (e.g., ISPs)? When is such cooperation needed?
- How and to what extent, if any, should active cyber defense be a coordinated effort for all systems that are attacked? (or is active cyber defense primarily applicable on an individual system basis?)
- What are the respective roles of the military, the intelligence community, and law enforcement authorities in active cyber defense?
- What changes, if any, should be made in existing legal regimes to facilitate active defense if active cyber defense is desirable?