Explorations in Cyber International Relations

Massachusetts Institute of Technology Harvard University

Perspectives On Cybersecurity: A Collaborative Study

Nazli Choucri

Political Science Department
Massachusetts Institute of Technology

Chrisma Jackson

Political Science Department
Massachusetts Institute of Technology

2015

This material is based on work supported by the U.S. Office of Naval Research, Grant No. N00014-09-1-0597. Any opinions, findings, conclusions or recommendations therein are those of the author(s) and do not necessarily reflect the views of the Office of Naval Research.

Citation: Choucri, N., & Jackson, C. (Eds.). (2015). *Perspectives on cybersecurity: A collaborative study* (ECIR Working Paper No. 2015-1). MIT Political Science Department.

Unique Resource Identifier: ECIR Working Paper No. 2015-1.

Version: Author's final manuscript.

Explorations in Cyber International Relations

Massachusetts Institute of Technology Harvard University

PERSPECTIVES on CYBERSECURITY

A Collaborative Study

Authors

Chrisma Jackson

Lyla Fischer

Brooke Gier

Vivian Peron

Ben Ze Yuan

Liu Yangyue

Glenn Voelz

Editors

Nazli Choucri

Chrisma Jackson

Department of Political Science

MIT

2015

Electronic copy available at: https://ssrn.com/abstract=2734336

Table of Contents

Electronic copy available at: https://ssrn.com/abstract=2734336

1. Cybersecurity – Problems, Premises, Perspectives

Nazli Choucri and Chrisma Jackson

1.1 Introduction

Almost everyone recognizes the emergence of a new challenge in the cyber domain, namely *increased threats to the security of the Internet and its various uses.* Seldom does a day go by without dire reports and hair raising narratives about unauthorized intrusions, access to content, or damage to systems, or operations. And, of course, a close correlate is the loss of value. An entire industry is around threats to cyber security, prompting technological innovations and operational strategies that promise to prevent damage and destruction.

Explanations as why cybersecurity has attained such a high degree of salience are far greater than is our understanding of the basic parameters in any matter touching on security, at all levels of analysis, namely: *who does what, when, why, how, and with what effect.* Most of the time it is possible to reconstruct the damage-episode and develop some hypotheses about several of the basic factors. But seldom, if ever, do we obtain a full reconstruction of the episode in all of its manifestations.

Unexpected as it is, nonetheless, we recognize the limits of our knowledge, the absence of robust understanding of the dynamics at hand, the paucity of theoretical or policy, and the list goes on. Even more compelling is the absence of an agreed upon definition of cybersecurity that encompasses the domain at hand, the conditions that undermine our confidence in cyber systems, and views as to the post threat realities and responses. All of this is a tall order indeed. While information of damage-episodes is amply, the data are not available in ways that allow for cumulative assessments. We still at a very early stages of systematic analysis.

This chapter is an introduction to a "reasoning exercise" designed to help clarify some of the more fundamental elements that constitute the emergent challenge of cybersecurity. Undertaken in the context of a new course on *Cybersecurity* in the Department of Political Science at MIT, this initiative spans a wide range of fundamental issues. The authors of the individual chapters, all participants in this course, provide foundational insights and evidence that, jointly, contribute to the help us to "fill in" some of the "many blanks" referred to above.

In this introduction we begin with a simple example to illustrate the reasons surrounding ambiguity or absence of definition, as well as what might be some attendant implications. Then we highlights, in a sentence or two, the contributions of each of the essays that follow.

1.2 The Cyber Domain: Alternative Views

Our "reasoning excessive" was designed as a multidisciplinary and multidimensional initiative and, to the extent possible, empirical grounded and policy relevant. In the absence of a

Electronic copy available at: https://ssrn.com/abstract=2734336

viable starting point, we fell back on the most obvious, namely, the nature of the cyber domain. It became immediately clear that, even in this small group, the diversity of views were such as to reinforce the cleavages in prevailing knowledge rather than the commonalities.

Put differently, at least three different "definitions" of cyberspace were put forth. Here we do not intend to argue that one was correct or that others were not. Rather our purpose is to signal that, given the derivative nature of cybersecurity, how we begin to address this complex issue might well shape what we "see" and decide to "do" about it. What we "see" is inevitably embedded in our understanding of cyberspace.

We now present the three views, with all the accompanying caveats and qualifiations.
But the underlying logic for the comparison remains importrant for the remainder of the "reasoning exercise"

First is the *technical focus*, put forth as the engineer's view, in Figure 1.1 below. All of the properties noted are critical and relevant. These may be necessary but are they sufficient to help shape effective framing of "cybersecurity". If so how? If not why not?

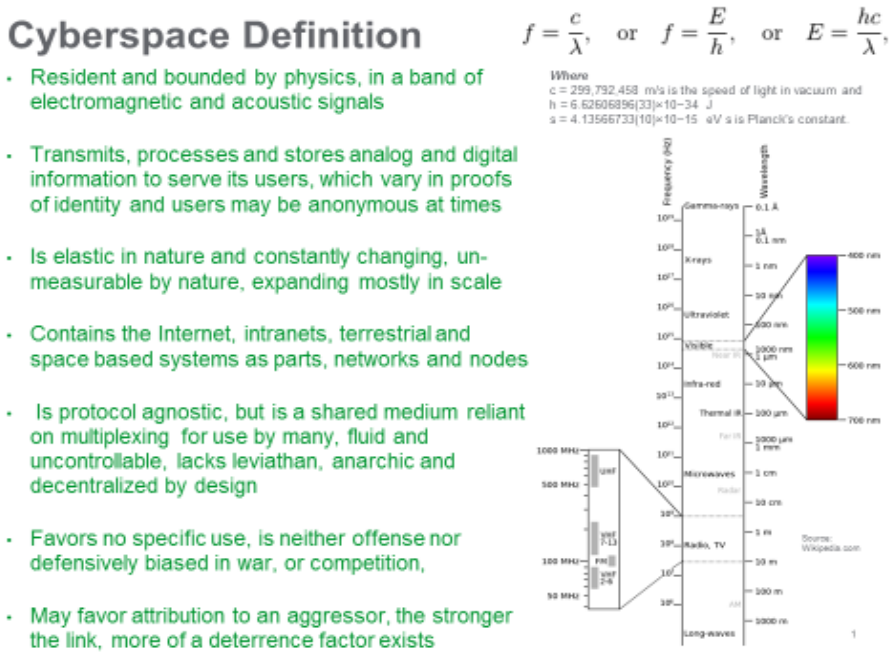


Figure 1.1
Source: George Wren. MIT Cybersecurity Seminar, Spring 2015.

Second is the *content focus.* Without undermining the technical infrastructure and underpinnings, this perspective on cyberspace broadens the framing and structures it around matters of information. As with the first focus, it is reasonable to state that all the features in future 1.2 may be necessary, but are they sufficient to help framing cybersecurity? If so how? If not why not?

Electronic copy available at: https://ssrn.com/abstract=2734336

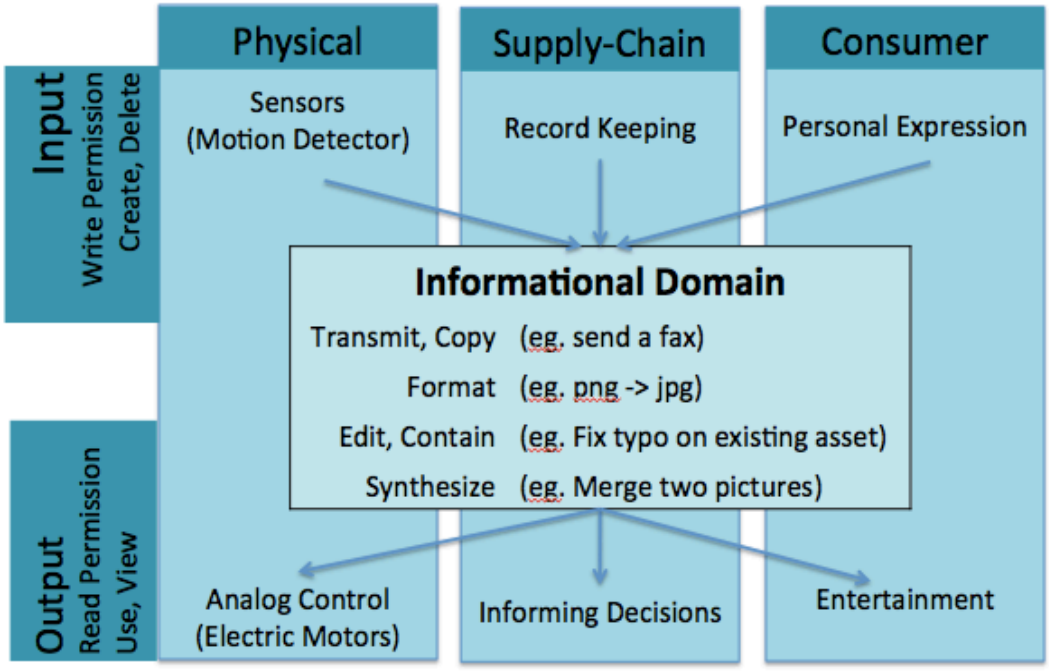


Figure 1.2
Source Lyla Fisher, MIT Cybersecurity Seminar, 2015.

Third is the *global view* this view sees cyberspace as a constructed domain of interaction. Shown in Figure 1.3 its scale and scope is greater than the first and second views. But we must still ask the question: These features are all necessary but are they sufficient to help frame "cybersecurity?

CYBERSPACE
Global Domain of Human Interaction

- Created through the interconnection of millions of computers by a global network such as the Internet.
- Built as a layered construct, where physical elements enable logical frameworks of interconnection
- Permits the processing, manipulation, exploitation, augmentation of information, and the interaction of people and information.
- Enabled by institutional intermediation and organization
- Characterized by decentralization and interplay among actors, constituencies and interests.

Figure 1.3

Electronic copy available at: https://ssrn.com/abstract=2734336

Source: Nazli Choucri , MIT Cybersecurity Seminar, Spring 2015

Each of these perspectives focuses on different manifestations of the cyber experience. It should come as no surprise that there are differences, or that the in the best of all possible worlds, the conception of cybersecurity derived from each of the above should be mutually supportive and integrative rather than mutually exclusive and competitive. Interestingly, each appears to be predicated on different phases in the construction and diffusion of the internet worldwide.

The first view is clearly architecture based. It implies that the "solution" to the cybersecurity problem (however defined) is to be found in the design itself and that the "flaws" can be corrected in that context thus reduce threats to cybersecurity. This is a view that minimizes the human or the institutional and organizational elements, but it reminds us that during the early d e sign phase of the Internet matters of security were not salient. Of importance was building an operational global networld rather than a network that is operational, global, as well as secure.

Implied in the above is something of an explicit trade-off. But there was no tradeoff at the time, as there was no security issue at stake then. Interstingly, cybersecurity became an issue as the global network extended its scale and scope, and users with different norms, values, and preferences took stock of the cyber possibilities and potential "venues" for pursuing their objectives. None of this reduces the value of the first view, rather it provides a contest for its importance.

The second view reflects the phase at which the Internet became reliable worldwide – at least relative to earlier experience – and content rather than reliability is viewed by users to be the central value. With increasing evidence unauthorized access – and the apparent ease with which this can be done – an added dimension of concern emerged, namely the protection of content. At this point, the Internet is no longer in "US hands" so to speak, but its very success as a revolutionary technology empowers others in ways that were not possible earlier.

And this leads to the consolidation of the third view. The proverbial "others" are conceivably anyone that has access to the Internet. And with this eventuality can a concern about the intent of those "others" as well as the sanctity of the global network and the reliability of the institutions established to manage different parts of the Internet and sustain its globalization.

This leads us to the following proposition: a coherent view of cybersecurity is one that spans conditions in the technical and operational domain, incorporates all matters of content, and extends its scope throughout the "supply chain". Here the notion supply chain is used in a figurative rather than literal sense. It refers, *at a very minimum*, to the properties of both structure and process "turned on" by user in the course of engaging in unauthorized access, the intents of the user, and the nature of the content accessed.

It goes without saying that concerns for cybersecurity are driven by the need to protect our own security in the cyber domain. Thus it may be important to distinguish between cybersecurity as the attribute of an actor versus an attribute of the global network as a whole. States and firms generally place their own self-interest first and foremost, and only if necessary do they find it relevant

Electronic copy available at: https://ssrn.com/abstract=2734336

to adopt a broader perspective.

The one critical implication of the above is that different actors are likely to view cybersecurity in different terms. The set of "ingredients" in the overall "mix" of concerns shaping their own conception of cybersecurity may have a common or shared core, or they might not. It is less important to resolve this matter than it is to better understand what might be the perspective of other actors. At this point in time, the salient "other" is China. It intents are suspicious and its capabilities are growing.

1.3 Perspectives on Cybersecurity

We now turn to the issues covered in the chapters that follow. With few exception, if any, they all derive from, or are connected to the forging, directly or indirectly. In this limited sense, then, we are moving toward a sense of "boundary" for the issue of cybersecurity.

Chapter 2 focuses on key technical issues. The purpose is to provide a "platform" that serves as foundations for understanding the technical functionalities essential for Internet operations and, by extensions, the potential targets for threat or damage. None of this issues addressed are contingent on a definition broader than the strictly technical features. Whatever is the definition of cybersecurity that assumed canonical status, it will most surely incorporate technical features.

Chapter 3 introduces conceptual issues that will, increasingly, feature into the cybersecurity debates. It is about the conceptual underpinnings of cybersecurity from the perspective of security studies. Today it is near-impossible to talk of national security without reference to threats in and of the cyber domain. This condition, driven by today's imperatives, requires conceptual and analytical underpinnings if it is to assume a position of credibility in policy analysis or in broader theoretical contexts. Such is the challenge addressed in this chapter.

Chapter 4 focuses on cyberspace as a domain of content. By way of orientation, it differentiates between the ends and means of cyberspace so that policymakers can focus on the ends and experts can specialize in the means. This perspective has implications for emergent conceptions of cybersecurity given that it is the security of content that dominates.

The next two chapters can be viewed as parallel perspectives. Chapter 5 is on cybersecurity seen by the US Department of Defense and Chapter 6 is about how China considers matters of cybersecurity and how it defines its key parameters. It is fair to say that these are far from mirror images of each other. Each reflects distinctive concerns. If there is a simple way of characterizing the US and the China perspective, it may be this: the US focuses on matters of process. China concentrates on features of structure. However unsatisfactory this distinction most surely is, nonetheless it captures some features of the differences between the two countries' conceptions of imperatives for cybersecurity.

Chapter 7 and Chapter 8 each take on the issue of deterrence in the cyber context. Is there a place for deterrence conventionally understood in the context of cybersecurity? Chapter 7 provides an initial mapping of the issues at hand. Labelled as a "discussion" of deterrence in the cyber era, this

Electronic copy available at: https://ssrn.com/abstract=2734336

chapter outlines some of the major features or perhaps fault lines in debates and deliberations. Chapter 8 simply asks: “Is deterrence possible in cyber warfare?”

Chapter 9 provides a major shift in focus, idiom, orientation, methodology, and inference space. Puts forth a theoretical framework for analyzing interactions between transitional activism and digital communication. While the connection to cybersecurity may not be immediately obvious from this statement of focus, the fact remains that any cross border source of cyber threat is, by definition, transitional in the strict sense of the term. At the same time, transitional activism refers to a form of political activity that is organized across borders without reliance on the role of direction of the state system.

Inevitably, this chapter reminds us that, however tempting it might be, we cannot ascribe all incidents of cyber intrusion to state actors. But the motivations are multiple. Threats to cybersecurity in business and industry are likely come as much from other states than from competitors in the marketplace. But the responses by the state are different from those by business, private or public. The fact remains, however, the data are inconclusive about sources, motivations and so forth. What we are more confident about is the nature of the intrusion and, more often than not, the immediate impacts on the target.

2. An Abbreviated Technical Perspective on Cybersecurity

Ben Ze Yuan

2.1 On Cyberspace

Understanding a view of cyberspace “from the ground” is a prerequisite to understanding the mechanics of offense and defense in the space. At a basic level, cyberspace owes its existence to that of its constituent machines - personal computers, servers, and embedded devices alike - connected by communication links to form interconnected networks. This graph topology provides the fabric on which all cyberspace activities are conducted - from the most mundane, like Web browsing and social networking, to the most sensitive, like financial transactions and business operations.

Every participant in cyberspace, even individual users, operates at least one network of their own, which may be as small as a single computer, or may be as large as a multi-million-node datacenter. These networks are interconnected by many types of links - directly by wired and wireless data links, and indirectly by human actions.

Cyberspace is a domain facilitating many different ends, and many of its applications expose things worth protecting to new risks. Individuals take on new risks to personal safety, financial assets, and personal reputation; corporations, too, must balance threats to revenue streams, intellectual property, and corporate reputation among customers. Increasing exposure to cyberspace implies an increasing degree to which a malicious actor can inflict damage of some type.

Electronic copy available at: https://ssrn.com/abstract=2734336

Exposure to the risks of cyberspace can be quantified, to a limited degree, based on the degree of separation of the "greater cyberspace" from the goals of an attacker. In some systems, it is possible to draw 'perimeters' or 'boundaries' based on where the amount of separation decreases; these boundaries are often located at the extents of system or network defenses, within which the degree of actual control on actions diminishes. In the modern world, however, these boundaries are fluid and more difficult to define. Employee actions taken to increase convenience, like remote access to corporate networks, may extend the perimeter in undesirable ways. Additionally, it is increasingly common to run business applications, store sensitive files, and even run entire virtualized networks, on top of third-party hardware, in which case the perimeter extends to that of the third party.

2.2 On Methods of Offense in Cyberspace

Aggressor parties operate with a variety of goals in mind, depending on their affiliations. State-actor aggressors may operate with military, industrial, or political objectives in mind, aiming to extract actionable intelligence, send a political message, or disable or destroy targets directly. Non-state actors may have an even broader spectrum of goals: individuals and non-state groups may act purely to further their own skills and prestige, or to achieve personally, financially, or politically motivated goals, or purely to pursue opportunistically available gains. Nevertheless, aggressor parties in cyberspace all leverage similar techniques in the process of working toward their own individual ends.

2.3 Denial of Service

The term 'denial of service' can refer to any action that prevents a service from working as intended, but is most commonly applied to actions that do so by sheer weight of traffic. The best-known technique is the distributed denial of service attack (DDoS), which leverages the traffic of thousands to tens of thousands of compromised machines to send so many requests at a computer or service that the target can no longer serve legitimate traffic. While denial-of-service can be seen as a crude, blunt instrument, and is indeed viewed as a last-resort technique for otherwise unsuccessful attackers, it is often effective at achieving certain goals - including both the obvious effect of disabling a system's ability to serve legitimate requests from the larger Internet, a perfectly legitimate end state, and the effect of diverting defender attention away from other systems.

Of note is the observation that certain nation-states are uniquely positioned to use denial-of-service as an offensive strategy. For instance, China, with its access to nearly 700 million Internet users and a demonstrated capability to leverage cross-border traffic as an attack mechanism is fully capable of using denial-of-service at scale to achieve political goals, as well as potentially able to leverage the capability against other types of targets.[1]

[1] Bill Marczak, Nicholas Weaver, Jakub Dalek, Roya Ensafi, David Fifield, Sarah McKune, Arn Rey, John Scott-Railton, Ronald Deibert, and Vern Paxson. 2015. "China's Great Cannon," *University of Toronto Munk School of Global Affairs* Research Brief, April. https://citizenlab.org/wp-content/uploads/2009/10/ChinasGreatCannon.pdf.

Electronic copy available at: https://ssrn.com/abstract=2734336

2.4 Exploitation of Software Vulnerabilities

Building truly secure software is a hard problem; any sufficiently large piece of software will have bugs, i.e. behavior inconsistent with expectations, and some of these bugs will result in vulnerabilities, i.e. opportunities to violate the abstractions assumed by the design of the system. Depending on the scope of the vulnerabilities and the capabilities afforded to a malicious party, the implications may range from trivial to catastrophic.

The prevalence of the Web as an application platform assures the attractiveness of discovering and exploiting vulnerabilities in Web applications. The classic examples are SQL injection, or database access enabled by application failure to properly sanitize data, and cross-site scripting, or the ability to deploy malicious JavaScript of an attacker's choice by promulgating a carefully crafted URL or by persistently injecting code into a webpage. Both of these techniques leverage faulty assumptions in a Web application's code to achieve otherwise unanticipated effects. SQL injection enables reading and writing of an application's database, allowing direct manipulation and harvesting of credentials and other sensitive data; cross-site scripting enables execution of code in local page scope, allowing an attacker to steal information or impersonate users.

One recent trend in Web attacks is to attack the TLS (Transport Layer Security) protocol itself rather than a Web application directly.[2] TLS uses strong encryption to protect high-value transactions from both passive eavesdropping and active attack, so any attack against TLS can reveal valuable information, like credentials, encryption keys, personal identity information, and financial data. Misconfiguration of TLS - for example, supporting weak cipher suites, or supporting the obsolete SSLv2 protocol - creates leverage points an attacker can use to attack individual sessions. More interestingly, bugs in implementations of TLS - like the infamous 'Heartbleed' vulnerability - can create opportunities for attackers to steal encryption keys and use them to impersonate a target server or decrypt traffic directly.

The most 'powerful' remote exploits, in terms of capability immediately afforded, are those that afford an attacker with remote code execution, i.e. the ability to run code of its choice, especially in a trusted context. Remote code execution effectively gives an attacker a measure of direct control over a target machine. From such a foothold, an attacker can manipulate the compromised service directly, attempt to establish greater control over the system, or use the capability to investigate other systems on the same network from an internal pivot point.

2.3 Social Engineering

In principle, even if not in practice, it might be possible to construct a system that implements a set of security rules perfectly - but such a system would necessarily exclude humans, who are comparatively unreliable yet often have the privilege or ability to override or circumvent security rules entirely. Social engineering describes the art of manipulating humans to accomplish a particular

[2] Symantec Corporation, "Internet Security Threat Report, Volume 20," *Symantec Corporation* Technical Report 2015. https://www4.symantec.com/mktginfo/whitepaper/ISTR/21347932_GA-internet-security-threat-report-volume-20-2015-social_v2.pdf.

Electronic copy available at: https://ssrn.com/abstract=2734336

aggressor goal.

Email is a common vector of social engineering attacks because of its ease of mass parallelization and its inbuilt capability to deliver desired payloads through email attachments. The most common social engineering attack is probably the ’phishing’ email, which aims to convince a target to directly divulge sensitive information like account credentials and payment card details, or to send money directly under false pretenses, or to run code of the attacker’s choice disguised as a desirable program. Phishing emails are commonly massively parallelized in cases where attackers are interested in any potential target rather than specific objectives. However, they may be custom-tailored to specific targets to conduct “spear phishing”, using information gleaned from other methods about a specific organization or specific individuals to increase message credibility, often with the objective of targeting high-level executives and administrators. With email, attackers can often achieve their goals directly, or at least breach conventional controls, without ever challenging the perimeter defenses directly.

Social engineering attacks are not limited to email as a vector. Telephone calls are also a known vector for gathering sensitive data or coercing a target to take particular actions. Physical on-site activities are also a known vector; by posing as an employee or authorized contractor, an aggressor can achieve direct physical access to sensitive systems. Additionally, social engineering attacks need not be sophisticated at any level, technical or otherwise: an aggressor can merely ask up-front for a particular action to be conducted, under the presumed (or actual!) threat of consequences imposed by the aggressor or by a powerful organization.

In every case, social engineering takes advantage of human malleability, coupled with human ability to override technical controls. Direct defense against social engineering attacks consists of teaching personnel to recognize them and to challenge such attacks when necessary, but ensuring compliance on an organizational scale remains challenging.

2.5 Post-exploitation Activities

Once attackers have access to a system, they can conduct further actions to achieve their goals. If the compromised system is the location where the goal resides, then the attacker can often complete its objectives immediately; if the attacker’s access is restricted, it can often exploit operating system bugs or vulnerabilities in system services to achieve complete control in a process called ’privilege escalation’.

If the target network is particularly large, and the attacker’s foothold is on the periphery, then the attacker may need to move laterally through the network to find its objective. Attackers are aided in this task by the observation that network defenses are usually located at the periphery of a network, and internal controls tend to be much weaker due to implicit trust between computers on the same network. Attackers are also aided by the fact that credentials are often reused by the same person for multiple purposes on multiple machines; one set of compromised credentials can often provide easy access to an entire network.

Electronic copy available at: https://ssrn.com/abstract=2734336

The end goals of attackers vary, as do the final-stage actions required. Attackers seeking to extract valuable data from a network must exfiltrate it to a remote position without triggering any systems designed to detect such activity. Attackers seeking to destroy data can, of course, do so in place. Attackers can also use compromised machines as 'zombies' with which to attack unrelated targets from behind a layer of indirection; this may be done at scale by building and using a 'botnet', or entire collection of compromised machines.

One interesting trend is the rise of ransomware, specifically crypto ransomware, which encrypts files in place and then demands payment of a fee through trace-resistant means for decryption. This method is an interesting means of accomplishing data destruction against parties unwilling to pay, and accomplishing extraction of funds against other parties. The actual amount extracted per target is relatively small - on the order of a few hundred USD - but the payload may be delivered at massive scale through cross-site scripting or phishing campaigns, allowing significant revenue for the authors of such payloads even with a relatively low conversion rate. Of note is the fact that such payloads have had success even against law enforcement agencies, traditionally instruments of the state, exemplifying the reality that non-state actors can often achieve damaging effects in cyberspace against state actors even without access to sophisticated techniques.[3]

There is a class of post-exploitation activities commonly associated with actors with advanced capabilities. Independent researchers have demonstrated the feasibility of causing direct kinetic effects on computers themselves, physically damaging them to the point of nonfunctionality.[4] Additionally, previous cyberattacks, like the well-known Stuxnet attack discovered in 2010, have demonstrated the feasibility of causing kinetic effects on devices attached to vulnerable computers. Such effects generally require close knowledge of the systems being attacked; such knowledge requires large expenditure of time by highly skilled individuals, and is thus easier to acquire for well-funded organizations, but is not necessarily the exclusive domain of state actors or even state-sponsored actors.

2.6 On the Methods of Defense

Defense in cyberspace is a challenging goal for multiple reasons. The most salient challenge to defense is its inherent difficulty in relation to even a single attacker; an attacker often needs only find a single vulnerability on a system to achieve its goals, while a defender aiming to keep all attackers out must anticipate every possible avenue of attack. This problem is magnified by the ease with which potential aggressors can achieve attack power, with the easy and wide proliferation of tools and knowledge, as well as the agility with which modern attackers can shift tactics. Additionally, the importance of proper defensive measures in relation to the risks remains challenging to describe to decision makers; high-quality defensive tools and services are expensive, and the return on investment is unclear due to the difficulty of quantifying the amount of damage thus avoided. Practices conducive to security also often remain a source of inconvenience for users, which thus themselves pose a

[3] Hiawatha Bray, "When hackers cripple data, police departments pay ransom," *The Boston Globe* April 6, 2015. https://www.bostonglobe.com/business/2015/04/06/tewksbury-police-pay-bitcoin-ransom-hackers/PkcE1GBTOfU52p31F9FM5L/story.html
[4] George Kurtz and Dmitri Alperovitch, "Hacking exposed: day of destruction," Presented at RSA Conference, San Francisco, February 26, 2014. http://www.rsaconference.com/writable/presentations/file_upload/exp-w01-hacking-exposed-day-of-destruction.pdf.

Electronic copy available at: https://ssrn.com/abstract=2734336

problem for compliance.

Solutions do exist to help provide security for a network. Firewalls and air gaps can prevent an attacker establishing a foothold in the first place. Intrusion detection systems can monitor anomalous activity throughout an entire network and alert decision makers. Antivirus systems can protect endpoints against known malware. Regular software updates can reduce the usefulness of 'prepackaged' exploits. Ultimately, however, these solutions can only increase the cost of an attack, and are of course, of limited value against an attacker capable of subverting such measures; there remains no adequate substitute for active response by a trained incident response team.

The value of defense in depth should not be discounted. Too often, an organization concentrates its defenses at the network perimeter, giving insufficient attention to internal controls that could slow or stop an attacker once the perimeter has been breached. Of course, defense in depth remains unfortunately expensive both from a development standpoint and from an operational perspective.

2.7 On the Accessibility of Attack Capability

Attack capability in cyberspace is by no means the sole domain of the state, as it arguably is in the physical world. In fact, many of the tools and techniques with which attack is conducted are freely available and freely shared. In the current state of cybersecurity, particularly with regards to the length of time a vulnerability can remain viable for exploitation, achieving a usable degree of attack power is not difficult for any actor with sufficient motivation and skill.

At the most basic level, attack power can be bought or rented. Popular exploit kits like Sakura, SpyEye, and Blackhole may be readily leased for a few hundred USD; these are kept up-to-date by their authors, who compile large collections of known exploits that may simply be tried *en masse* against targets.[5] While individual exploits may diminish in value after being patched and updated, the diversity in update schedules and the sheer breadth of exploits used in a given kit increase the probability that at least one usable exploit can be found against any given target. Exploit kits are also engineered for usability by people with limited technical ability, and technical support is often available with the purchase price. While these kits are marketed towards cybercrime, with the aim of extracting marketable goods like credit card numbers, email credentials, and identity documents, they can be adapted for other purposes against vulnerable targets.

Exploits, of course, must be discovered, and this task remains the domain of highly skilled, highly trained individuals. However, the necessary tools - debuggers, compilers, packet analyzers, and the like - are freely available, and are also necessary tools for legitimate software development. Additionally, vulnerability discovery is a skill that may be readily learned through freely available study material and through paid courses, and has legitimate applications in securing software and systems. It is thus uncontroversial that an individual with a background in software engineering may take an interest in learning about security testing, and actual intent is difficult if not impossible to ascertain *a priori*.

[5] Symantec Corporation, "Internet Security Threat Report, Volume 20," *Symantec Corporation* Technical Report 2015. https://www4.symantec.com/mktginfo/whitepaper/ISTR/21347932_GA-internet-security-threat-report-volume-20-2015-social_v2.pdf.

Electronic copy available at: https://ssrn.com/abstract=2734336

2.8 Requirements and Difficulties for Control

In order to exert effective controls over cyberspace, credible means of applying force and the ability to identify appropriate targets are both required. Credible force need not be restricted to the cyber realm; retaliation against a cyberattack may very well take the form of more traditional law enforcement or military techniques. Identification of appropriate targets is a more challenging problem because of the difficulty of attribution.

Attribution in cyberspace is tricky. One challenge is the decoupling of physical identity and virtual identity: it is feasible for a person to maintain one or more virtual identities with very limited, if any, coupling with a real world identity. Another challenge is the degree to which attackers can leverage indirection, and the subsequent effects on attempts to reidentify them. Attackers can use “borrowed” machines to conduct their attacks, and hence identifying the ’machine of origin’ for a particular attack becomes a multi-step, possibly multi-national problem. Additionally, attackers can use “borrowed” tools, making identification based on fingerprinting of techniques less reliable. Traditional intelligence and law-enforcement techniques can still yield results when attackers exhibit lapses in operational security. However, it is not outside possibility for attacks to become so resistant to attribution that correctly implementing retributive measures becomes challenging at best.

One might seek to solve the attribution problem through aggressive technical measures, and indeed such an approach may yield gains for cybersecurity. However, the impacts of any such approaches on the free and open character of the current Internet, and on U.S.-friendly interests relying on anonymity for their own goals, must be weighed carefully. Additionally, implementing controls on the relevant knowledge or tools would seem like a fruitless or even counterproductive endeavor, due to the impact on current and future cyber talent; in fact, if anything, encouraging the proliferation of cybersecurity expertise may be a net benefit, in order to increase the talent base available to implement and improve existing defensive capabilities.

Electronic copy available at: https://ssrn.com/abstract=2734336

References

Bray, Hiawatha. 2015. "When hackers cripple data, police departments pay ransom," The Boston Globe April 6. https://www.bostonglobe.com/business/2015/04/06/tewksbury-police-pay-bitcoin-ransom-hackers/PkcE1GBTOfU52p31F9FM5L/story.html

Kurtz, George and Dmitri Alperovitch. 2014. "Hacking exposed: day of destruction," Presented at RSA Conference, San Francisco, February 26. http://www.rsaconference.com/writable/presentations/file_upload/exp-w01-hacking-exposed-day-of-destruction.pdf.

Marczak, Bill, Nicholas Weaver, Jakub Dalek, Roya Ensafi, David Fifield, Sarah McKune, Arn Rey, John Scott-Railton, Ronald Deibert, and Vern Paxson. 2015. "China's Great Cannon," University of Toronto Munk School of Global Affairs Research Brief, April. https://citizenlab.org/wp-content/uploads/2009/10/ChinasGreatCannon.pdf.

Symantec Corporation, 2015. "Internet Security Threat Report, Volume 20," Symantec Corporation Technical Report. https://www4.symantec.com/mktginfo/whitepaper/ISTR/21347932_GA-internet-security-threat-report-volume-20-2015-social_v2.pdf.

.

Electronic copy available at: https://ssrn.com/abstract=2734336

3. The Conceptual Underpinning of Cyber Security Studies

Liu Yangyue

Technology is often a driving force in the transformation of the international system. Over the past two decades, such transformative power has been best manifested in the development of information technologies, which are adjusting and reshaping the "interaction capacity" of human society.[6] An important part of this change occurs in the security domain. Development of the Internet and related technologies has empowered new political actors, fostered new patterns of interactions, and also opened up new venues for threats and conflicts. This security aspect of cyber politics becomes even more salient, as human reliance upon cyberspace intensifies. How the advent of cyberspace influences the meaning and conduct of security practices has sparked increasing academic interest and increasing discussion since 2007 (Figure 1).

There are abundant discussions in security studies and international relations about the emerging risks and challenges associated with cyberspace. However, partly due to the complexity of the new socio-technological system, little consensus has been reached on what constitutes cyber security. On this score, Hansen and Nissenbaum pointedly remarked that "in spite of the widespread references to cyber insecurities in policy, media, and Computer Science discourses, there has been surprisingly little explicit discussion within Security Studies of what hyphenating 'security' with 'cyber' might imply".[7]

Therefore, this review attempts to examine the burgeoning literature on cyber security, mainly from an international security study (ISS) perspective. ISS represents a research field that concerns different types of actors, as well as different levels of policy responses, in international politics. The emergence of cyber security issues adds a new, yet important, dimension to this field. But, it also raises a serious question of how this unprecedented cyber phenomenon should be conceptualized and measured.

[6] Barry Buzan, Charles Jones, and Richard Little, *The Logic of Anarchy: Neorealism to Structural Realism* (New York: Columbia University Press, 2009)
[7] Lene Hansen and Helen Nissenbaum, "Digital Disaster, Cyber Security, and the Copenhagen School," *International Studies Quarterly* 53 (2009): 1156.

Electronic copy available at: https://ssrn.com/abstract=2734336

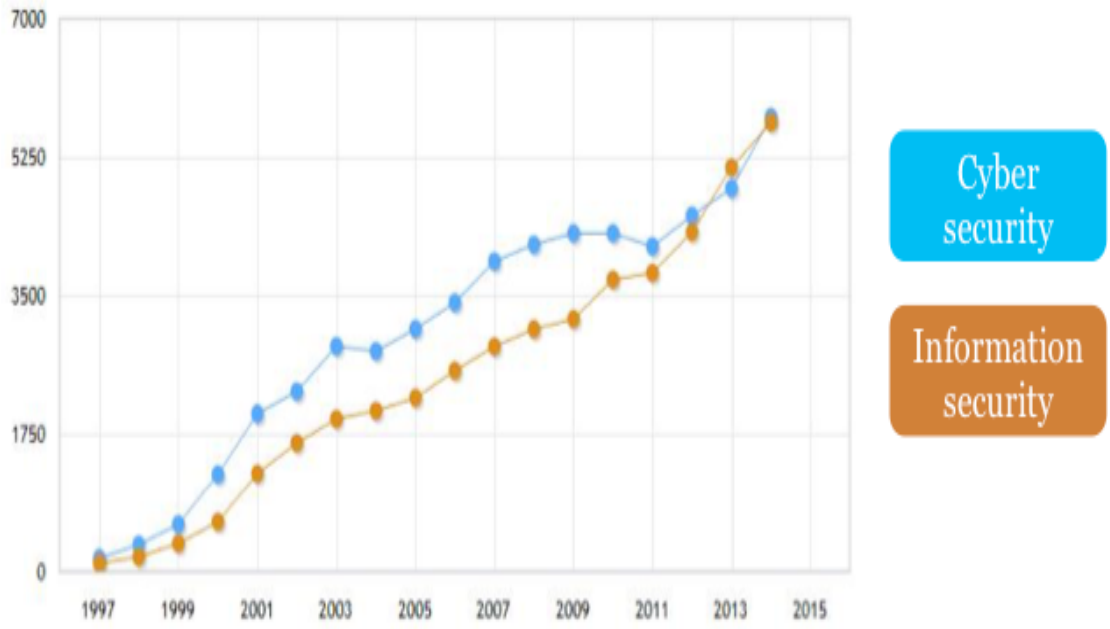


Figure 3.1
Burgeoning Discussions on Cyber Security

3.1 Cyber Security in the Broad Context of International Security Studies

Starting from the later years of the Cold War, the discipline of international security studies has experienced a dual shift on its agenda.[8] On the one hand, the previously narrow focus on military-political security is expanded to include other sectors such as economic security and environment security. The 1994 *Human Development Report* published by the United Nations Development Programme suggested that the scope of global security should be extended to threats from economic, food, health, environmental, personal, community and political areas.[9] It also identified the significant linkage between development and security, thus broadening the conceptual boundary and policy orientations of security studies.[10] Accompanying these "widening" efforts is a growing list of non-traditional threats and risks such as terrorism and global pandemics. Security problems caused by the use of computers and digital networks make their appearance on that list, too.

Although these problems were considered purely technical at the beginning, the increasingly intertwining relationship between cyber domain and other sources of threats – both traditional and non-traditional – has attached much greater significance to cyber security.[11] Meanwhile, the constructed notion of cyberspace, with an imagined resemblance to other geographic space (sea, air,

[8] Barry Buzan and Lene Hansen, *The Evolution of International Security Studies* (Cambridge: Cambridge University Press, 2009).
[9] United Nations Development Programme, *Human Development Report* (New York: Oxford University Press, 1994).
[10] Caroline Thomas, "Global Governance, Development and Human Security: Exploring the Links," *Third World Quarterly* 22 (2001): 159-175; Pauline Ewan, "Deepening the Human Security Debate: Beyond the Politics of Conceptual Clarification," *Politics* 27 (October) 182-189.
[11] Johan Eriksson and Giampiero Giacomello, "The Information Revolution, Security, and International Relations: (IR) Relevant Theory?," *International Political Science Review* 27 (2006): 221-244.

Electronic copy available at: https://ssrn.com/abstract=2734336

outer space etc.), implicates a perceivable domain that can be both target and source of security risks.[12] As noted by Buzan and Hansen, technological changes and key events are among the major driving forces of security studies.[13] Similar mechanisms may also apply to cyber security. In this sense, the meaning of security in cyberspace would not remain static, subject, instead, to the dynamics of technological development and unforeseen circumstances.

On the other hand, "wideners" of international security studies are joined by "deepeners" who stress the need to move beyond the nation-state as the sole "referent object" of security. The critical question of "security for whom" highlights vulnerabilities of non-state entities – individuals, groups, communities – who suffer violence from various levels of threats. By extending security objects vertically, it should be regarded as an integral part of the human security narrative as well as the security-development nexus.[14] In addition, this approach indicates that providers of security services become multiplied and security is not a public good offered and realized only by the state apparatus.[15] Again, discussions on cyber security parallel and exemplify these "deepening" efforts. As interactions in and through cyberspace effectively connect all levels of actors and systems, it is difficult to speak of security without referring to users, corporations, organizations, processes, and systems, all of which, alongside states, are essential components, and thus security objects, of cyberspace. New modes of security governance also take shape, delegating power from traditional, hierarchical structure to networked, decentralized collaboration.[16]

Therefore, the perceptions of cyber security issues have, in general, conformed to the evolution of international security studies. But it also means that the process of knowledge generation on cyber security would be influenced by existing vocabularies, theories, frameworks and mindsets of international security studies, yet leaving the validity of such "concept travelling" unexplored.[17] Typical examples can be found in the coined terms such as "cyber war" and "cyber weapon", or in the biological analogies of computer viruses and worms.[18] Still under debate is to what extent these metaphors can deliver accurate connotations to cyber-related phenomenon.

3.2 Sources of Cyber Threats

Despite its various meanings, security is foremost understood as the status or value of being free from threats.[19] As Ullman put it, "we may not realize what it (security) is or how important it is until we are threatened with losing it".[20] As a result, defining security often pertains to identifying and describing threats that challenge it.

---

[12] Ronald Deibert and Rafal Rohozinski, "Risking Security: The Policies and Paradoxes of Cyberspace Security," *International Political Sociology* 4 (2010): 15-32.
[13] Buzan and Hansen, *The Evolution of International*, 53-57.
[14] Barry Buzan, Ole Wæver, and Jaap de Wilde, *Security: A New Framework for Analysis* (Boulder, CO: Lynne Rienner Publishers, 2009); Gary King and Christopher Murray, "Rethinking Human Security," *Political Science Quarterly* 116 4 (2001): 585-610; Maria Stern and Joakim Öjendal, "Mapping the Security-Development Nexus: Conflict, Complexity, Cacophony, Convergence?," *Security Dialogue* 41 (2010): 5-29.
[15] Lucia Zedner, *Security*, (London: Routledge, 2009).
[16] Milton Mueller, Andreas Schmidt, and Brenden Kuerbis, "Internet Security and networked Governance in International Relations," *International Studies Review* 15 (2013): 86-104.
[17] Giovanni Sartori, "Concept Misformation in Comparative Politics," *American Political Science Review* 4 (1970): 1033-1053.
[18] Thomas Rid, *Cyber War Will Not Take Place*, (Oxford: Oxford University Press, 2013); David J. Betz and Tim Stevens, "Analogical reasoning and cyber security," *Security Dialogue* 44 (2013): 147-164.
[19] Arnold Wolfers, ""National Security" as an Ambiguous Symbol," *Political Science Quarterly* 67 (1952): 481-502; Richard H. Ullman, "Redefining Security," *International Security* 8 (1983): 129-153.
[20] Ullman, "Redefining Security," 133.

Electronic copy available at: https://ssrn.com/abstract=2734336

The understanding of cyber security starts with a similar pattern. When the earliest known computer virus (codenamed Morris Worm after its programmer) infected thousands of computers in the United States and overseas, a report by US General Accounting Office (1989) several months later warned the government of the security vulnerabilities exposed by the Internet virus and other intrusions. The first Computer Emergency Response Team was established immediately after the incident, with one of its major functions being the provision of "mechanisms for coordinating community response in emergencies, such as virus attacks or rumors of attacks".[21] During those early days, the primary concern of cyber-related security centered on the potential loopholes of computer systems, which might lead to loss or leakage of computer data and problems of computer crime.[22] The same vulnerability that permitted a virus attack by malicious individuals was thought to be likely exploited by terrorists and foreign nations. In this regard, the US National Academy of Sciences cautioned in 1991 that "tomorrow's terrorist may be able to do more damage with a keyboard than with a bomb".[23] Though visionary, these accounts fell short of presenting any detailed scenario of a future threat.

The National Institute of Standards and Technology, in its 1995 *Introduction to Computer Security*, further specified nine types of security threats, including errors and omissions, fraud and theft, employee sabotage, loss of physical and infrastructure support, malicious hackers, industrial espionage, malicious code, foreign government espionage, and threats to personal privacy. It mainly underscored the risk of interception of, or illegal access to, digitized data, while pointing to various kinds of perpetrators.[24] As the development of information technologies fosters greater penetration of the Internet into human society, perceptions of cyber threats naturally expand, and the relatively narrow sense of computer security evolves into a more inclusive notion of cyber security.

Accordingly, sources of security threats proliferate. Now cyber security is seen as encompassing a host of problems, such as spamming and phishing, unauthorized intrusions, denial-of-service attacks, website defacements, online surveillance, unintended bugs in protocols and systems, as well as the intersection with military and political threats.[25] The list of cyber threats is largely expandable, especially as new threats emerge from the increasingly digitalized and interconnected physical domain. Examples include security concerns to the cyber-physical systems, supervisory control and data acquisition (SCADA) networks, and even unmanned aerial vehicles (UAVs).[26] Some

[21] Jason Healey and Karl Grindal, eds., *A Fierce Domain: Conflict in Cyberspace, 1986 to 2012* (Vienna, VA: Cyber Conflict Studies Association, 2013.
[22] Myriam Dunn Cavelty, "Cyber-Terror-Looming Threat or Phantom Menace? The Framing of the US Cyber-Threat Debate," *Journal of Information Technology and Politics* 1 (2007): 24.
[23] National Academy of Sciences, *Computers at risk: Safe computing in the information age* (Washington, DC: National Academy Press, 1991).
[24] Barbara Guttman and Edward Roback, *An Introduction to Computer Security: The NIST Handbook* (Gaithersburg, MD: U.S. Department of Commerce, 1995).
[25] William J. Lynn III, "Defending a New Domain: The Pentagon's Cyberstrategy," *Foreign Affairs* 89 (2010): 97-108; Milton Mueller, *Networks and States: The Global Politics of Internet Governance* (Cambridge, MA: The MIT Press, 2010); Ronald Deibert, "The Growing Dark Side of Cyberspace(…and What To Do About It)," *Penn State Journal of Law and International Affairs* 1 (2012): 260-274; Derek S. Reveron, "An Introduction to National Security and Cyberspace," in *Cyberspace and National Security: Threats, Opportunities, and Power in a Virtual World*, ed Derek S. Reveron (Washington, DC: Georgetown University Press, 2012), 11-12; Brandon Valeriano and Ryan C. Maness, "The dynamics of cyber conflict between rival antagonists, 2001-11," *Journal of Peace Research* 51 (2014): 353-354.
[26] Md E. Karim and Vir V. Phoha, "Cyber-physical Systems Security," in *Applied Cyber-Physical Systems*, ed. Sang C. Suh, U. John Tanik, John N. Carbone, and Abdullah Eroglu (Switzerland: Springer, 2014); Eric Knapp and Joel T. Langill, *Industrial Network Security: Securing Critical Infrastructure Networks for Smart Gride, SCADA, and Other Industrial Control Systems*, (Rockland, MD: Syngress Publishing, 2011); Kim Hartmann and Christoph Setup, "The Vulnerability of UAVs to Cyber Attacks – An Approach to the Risk Assessment," in *5th International Conference on Cyber Conflict*, ed. K. Podins, J. Stinissen, and M. Maybaum (Tallinn: NATO CCD COE Publications, 2013).

Electronic copy available at: https://ssrn.com/abstract=2734336

studies contribute to the threat list by identifying specific means or tools used in particular incidents.[27] These threats appear to be progressively advanced and persistent, as they employ complicated techniques and operate in a long-term, systematic manner.[28] Myriam Dunn Cavelty further distinguished among three clusters of cyber threats: a technical cluster that concentrates on malware, a socio-political cluster that captures various human wrongdoings, and a human-machine cluster that produces threats through complex interactions.[29] But, the problem of overlap (especially between the socio-political cluster and the human-machine cluster) that this classification intends to address remains, to some extent, unabated.

A key difference among these various forms of cyber threats lies in their levels of severity (or intensity). It often argues that cyber threats can be classified according to the damage incurred, methods and actors involved, and motivations behind.[30] Thus, the mapping of cyber threats usually points to a spectrum with unintentional failures (such as software or system errors) – assumed as the least dangerous – at one end, and full-blown, strategic cyber warfare – perceived as the most destructive and destabilizing – at the other. In between the extremes are malicious activities initiated by criminals (in the name of cyber crime), spies (cyber espionage), terrorist groups (cyber terrorism), or other political organizations (cyber conflict)[31]. Though not articulated as direct security threat, cyber conflict also exists in political contention over the designing and management of cyberspace and its resources.[32] The gradual politicization of such contention would likely produce security implications for the relevant actors. On the military side of the cyber-threat continuum, differentiation can still be made among enabling operations (activities relating mostly to reconnaissance and intelligence collection), disruptive operations, and outright cyber attacks.[33]

The internal logic common in these efforts shares great similarities with Charles Tilly's seminal work on collective violence, which highlights (a) damage caused by and (b) degree of organized coordination among violent participants.[34] That said, classifying cyber threats by mapping a spectrum suffers several drawbacks. Firstly, threats and conflicts in a cyber context often involve a mixture of stakeholders.[35] It is difficult, for instance, to properly place attacks initiated by state actors against non-state actors (and vice versa) on a continuum, let alone those initiated by a combination of actors or involving ambiguous, mysterious cyber militias. The proliferation of political actors in cyberspace and the problem of attribution have, to some extent, blurred the division of cyber crime, terror, and

[27] James P. Farwell and Rafa Rohozinski, "Stuxnet and the Future of cyber War," Survival 53 (2011): 23-40; Christopher R. Hughes, "Google and the Great Firewall," *Survival* 52 (2010): 19-26.
[28] Mandiant, APT1: Exposing One of China's Cyber Espionage Units (2013): http://intelreport.mandiant.com/Mandiant_APT1_Report.pdf; James A. Lewis, "Cyber Threat and Response: Combating Advanced Attacks and Cyber Espionage," Center for Strategic & International Studies Report (2014).
[29] Myriam Dunn Cavelty, "From Cyber-Bombs to Political Fallout: Threat Representations with an Impact in the Cyber-Security Discourse," *International Studies Review* 15 (2013) 108-109.
[30] Jan-Frederik and Benedikt Müller, "SAM: A Framework to Understand Emerging Challenges to States in an Interconnected World," in *Cyberspace and International Relations: Theory, Prospects and Challenges*, ed. Jan-Frederik and Benedikt Müller (Switzerland: Spring 2014) 45-51.
[31] Myriam Dunn Cavelty, *Cyber-Security and Threat Politics: US Efforts to Secure the Information Age* (New York: Routledge, 2008) 20; Paul Cornish, Rex Hughes, and David Livingstone, *Cyberspace and the National Security of the United Kingdom: Threats and Responses* (London: Chatham House, 2009); Nicholas Thomas, "Cyber Security in East Asia: Governing Anarchy," *Asian Security* 5 (2009): 3-23; Nazli Choucri, *Cyberpolitics in International Relations* (Cambridge, MA: The MIT Press, 2012); M.A. Gregory and David Glance, *Security and the Networked Society* (Switzerland: Spring, 2013).
[32] Laura DeNardis, *Protocol Politics: The globalization of Internet governance* (Cambridge, MA: The MIT Press, 2009); Choucri, *Cyberpolitics*, 126.
[33] Gary D. Brown and Owen W. Tullos, "On the Spectrum of Cyberspace Operatins," *Small Wars Journal* December 11 (2012) http://smallwarsjournal.com/print/13595.
[34] Charles Tilly, *The Politics of Collective Violence* (Cambridge: Cambridge University Press, 2003).
[35] Kremer and Müller, "SAM", 44.

Electronic copy available at: https://ssrn.com/abstract=2734336

war. Secondly, while war represents the most destructive form of violence, current exercises of "cyber war" may qualify, more precisely, as forms of sabotage, espionage and subversion.[36] Meanwhile, cyber crimes inflict, so far, heaviest and most immediate harm on businesses and customers.[37] This calls into question the order of severity used as the criteria of a cyber threat spectrum. Last but not least, even among cyber threats involving distinctive clusters of actors and motives, methods and tools may still overlap. For instance, distributed denial-of-service (DDoS) attacks are found in all levels of cyber conflict, with botnets and other toolkits widely available in an underground economy.[38] Therefore, although pointing out the mounting sources of cyber threats would help to illustrate the diverse scenarios of security risks, it is still inadequate for a comprehensive understanding of the nature and characteristics of cyber security. A linear spectrum of cyber threats is problematic since it often relies on only one or two dimensions of threats (e.g. actors or severity), while leaving other dimensions (e.g. targets and intentions) and the intertwining effects among them unaddressed.

3.3 Boundary of Cyber Security

The notion of security often connotes a target at stake, be it a nation, a community, an individual, an asset, or anything else perceptible. The principal referent object – as securitization theory phrases it – of cyber security points to an artificial and imagined aggregation that connects human, information and machine through digital networks.[39] The coinage of cyberspace gives the collective objects a sense of reality and spatiality, albeit still virtual in nature, thus bringing it closer to the defense and protection narratives.[40] "When thinking about warfare, hackers, pornography, fraud, and other threats to the rule of law that pass through the internet", as Graham argues, "it is challenging to fully understand the complex geographies of these processes and practices.[41] It is much easier to imagine that they simply happen 'out there' in Carl Bildt's dark spaces of the internet". In this sense, the "consensual hallucination" of cyberspace is indeed a fundamental component of cyber security conceptualizations.[42]

However, when referring to cyberspace, studies on cyber security do not always share an identical, unambiguous definition. It is seldom a question that the ecological structure of cyber security consists of different levels (layers) of interactive dimensions. But disagreement arises, explicitly or implicitly, as to the exact composition of that structure. A dichotomous approach emphasizes the virtual-physical distinction of cyberspace, and the different (or even contradictory) security implications that result from its dual properties.[43] When cyberspace is used as the referent object of security, it primarily centers on the material domain – especially critical infrastructure – that suffers security risk and necessitates protection. Deibert and Rohozinski made a step forward by identifying "risks through cyberspace", which underscores the political challenges generated by activities in cyberspace.[44] These risks, composed of "resistance networks" and "dark nets", expand the

[36] Rid, *Cyber War*.
[37] Symantec, *Internet Security*.
[38] Jaideep Chandrashekar, Steve Orrin, Carl Livadas, and Eve Schooler, "The Dark Cloud: Understanding and Defending against Botnets and Stealthy Malware," *Intel Technology Journal* 13 (2009) 130-147; Farwell and Rohozinski, "Stuxnet", 23-40.
[39] Barry Buzan, Ole Wæver, and Jaap de Wilde, *Security*.
[40] Julie E. Cohen, "Cyberspace as/and Space," *Columbia Law Review* 107 (2007): 210-256.
[41] Mark Graham, "Geography/Internet: Ethereal alternate dimensions of cyberspace or grounded augmented realities?," *The Geographical Journal* 179 (2013): 179.
[42] William Gibson, *Neuromancer* (New York: Ace Books, 1984).
[43] Deibert and Rohozinski, "Risking Security," 15-32; Joseph S. Nye, "Nuclear Lessons for Cyber Security?," *Strategic Studies Quarterly* 5 (2011): 18-38.
[44] Deibert and Rohozinski, "Risking Security," 21-24.

Electronic copy available at: https://ssrn.com/abstract=2734336

referent objects of security from cyberspace to the broad socio-political order outside the cyber domain.

Other studies focus on cyberspace per se by dividing it into functional layers, but they still differ in how far these layers stretch. For instance, Libicki's trichotomy model of cyberspace posits a structure of the "physical" layer (primarily interconnected computers), the "syntactic" layer (software and protocols) and the "semantic" layer (information).[45] This structure would be both narrow and extensive when compared with other conceptions. Some of them regard cyberspace mainly as a technical system, thus merely focusing on the hardware and logical layers.[46] It is also narrow, since a broader structure of cyberspace may include the human/people dimension pertaining to the users of cyberspace, and the physical layer may not be restricted to digitally-connected computer systems.[47] Even air-gapped systems could be vulnerable to cyber attacks, and thus be considered as part of the cyber domain.[48] Moreover, in regard to the information layer, it would be crucial to distinguish between code and content of information. The latter often points to the perceptual aspect of human brain. It largely stretches the boundary of cyberspace to cover the subjective dimension associated with ideas, beliefs, and values.[49]

In general, there are two separate lines of boundary that govern the divergent conceptualizations of cyber security. One axis moves along the distinction between globalized space and imagined national boundary. The national side of this line of thinking does not necessarily end up with asserting national sovereignty over cyberspace, but it implicitly or explicitly portrays nation-states as the core referent object. Crucial factors that sustain the national image of cyber security point to the physical infrastructure of cyberspace which still operates within national borders, as well as the fundamental roles of territorial government that persist in the cyber domain.[50] The tendency to confine cyber security analysis within a state-centric framework is prevalent in studies from a strategic perspective, and evident in the documentation of national cyber security strategies outlined by a growing number of countries. On the other hand, cyber security represents a novel global issue that occurs in a new arena of interactions.[51] Norms, practices, and institutions that manage security problems in the cyber domain have been fundamentally transformed due to the globalized feature of the cyber system.[52] In this sense, confining discussions on cyber security within a national framework would be counterproductive, and the global governance of cyberspace indicates the de facto elimination of cyber security boundary. Meanwhile, the other line of conceptual boundary moves along the distinction between code and value that transmit in and through cyberspace. In general, stress on the code tends to highlight the technical system of cyberspace, while stress on the value tends to

[45] Martin C. Libicki, *Conquest in Cyberspace: National Security and Information Warfare* (Cambridge: Cambridge University Press, 2007).
[46] Kelce S. Wilson and Muge Ayse Kiy, "Some Fundamental Cybersecurity Concepts," *IEEE Access* 2 (2014): 116-124.
[47] Nazli Choucri and David Clark, Cyberspace and International Relations: Toward an Integrated System," Paper presented at Massachusetts Institute of Technology, Cambridge, MA: August 25, 2011; Shmuel Even and David Siman-Tov, "Cyber Warfare: Concepts and Strategic Trends," *The Institute for National Security Studies Memorandum* 117 (2012).
[48] Scott Applegate, "The Dawn of Kinetic Cyber," Presented at the *5th International Conference on Cyber Conflict*, Tallinn June 4-7, 2013.
[49] Keir Giles, "Russia's Public Stance on Cyberspace Issues," in *4th International Conference on Cyber Conflict,* ed. K. Podins, J. Stinissen, and M. Maybaum (Tallinn: NATO CCD COE Publications, 2012), 63-77.
[50] David Drezner, "The Global Governance of the Internet: Bringing the State Back In," *Political Science Quarterly* 119 (2004): 477-498; Jack L. Goldsmith and Tim Wu, *Who Controls the Internet?: Illusions of a Borderless World* (Oxford: Oxford University Press, 2006).
[51] Choucri, *Cyberpolitics*.
[52] John Mathiason, *Internet Governance: The New Frontier of Global Institutions* (London: Routledge, 2008); Nazli Choucri, Stuart Madnick, and Jeremy Ferwerda, "Institutions for Cyber Security: International Responses and Global Imperatives," *Information Technology for Development* (2013): DOI: 10.1080/02681102.2013.836699.; Mueller, Schmidt, and Kuerbis, "Internet Security".

Electronic copy available at: https://ssrn.com/abstract=2734336

underscore the social and political interactions embedded in the various processes that underpin cyber domain. Accordingly, four approaches to cyber security can be differentiated (Figure-2)

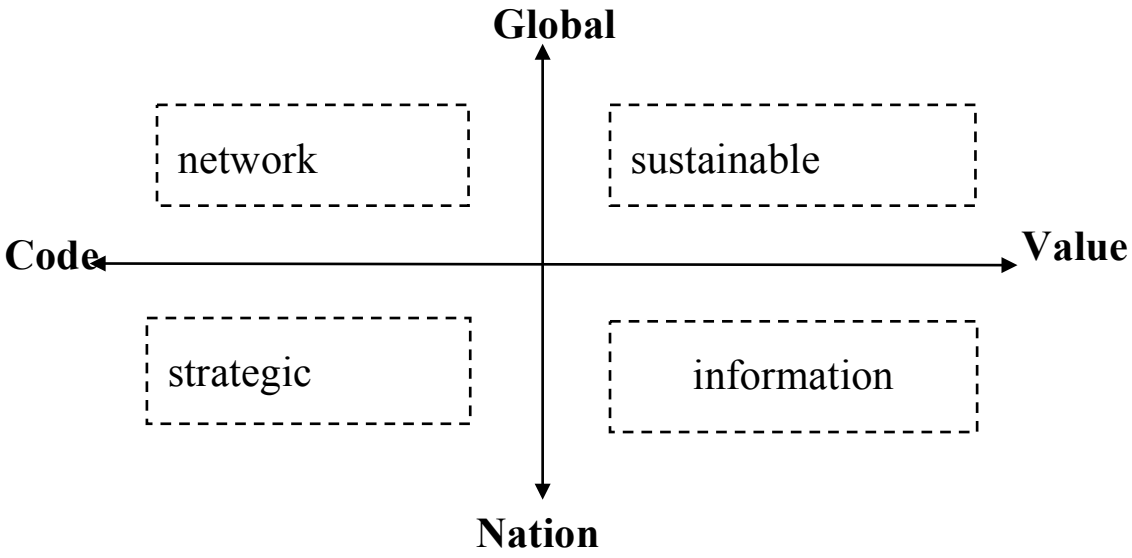


Figure 3.2
Approaches to cyber security

Network security in the upper left quadrant stresses the connectivity of cyberspace which is created through networked terminals and enabling technologies. The core for protection is a globalized network (global commons), which often calls for a horizontal (bottom-up) approach of security governance. By contrast, *strategic security* also underscores the connectedness of cyberspace, but at stake are national assets connected to the cyber domain. In this narrative, the foremost threat is malicious code used by state or non-state actors with strategic and political objectives. It pays special attention to the expanding intersection between cyberspace and military/strategic affairs. In the upper right quadrant, *sustainable security* focuses on the global system of cyberspace, but from a perspective highlighting distribution and development. The developmental objectives of human society are seen as being associated with the development and management of information sphere. This perspective is concerned with how cyber interactions are shaped by and regenerating, in return, human values. In this sense, management of cyber security should mitigate risks resulting from collisions between different values and interests. In *information security*, people and society within a nation-state define the boundary of cyberspace. It is focused primarily on the content and values embedded in information flows. The proposed response to cyber security often calls for regulations and norms on information content and human behavior. The existence of two separating lines (national-global and code-value) used to delineate cyberspace has, in some measure, enriched but also complicated our understanding and conceptualization of cyber security.

Moreover, the boundary of cyber security becomes further clouded as the result of international

Electronic copy available at: https://ssrn.com/abstract=2734336

power politics. It was observed in 2013 that the number of countries with more-or-less militarized cyber security programs had risen to 47.[53] Six of them publicly released their military cyber strategies, while another 30 expressed cyber security concerns in various national defense documents. However, these national strategies and policies diverge in their conceptualizations of cyberspace and cyber security. The most obvious contention can be found between Euro-Atlantic countries on the one hand, and countries such as Russia and China on the other.

The US Department of Defense defines cyberspace mainly by its technological (hardware) components, which describes the cyber domain as "the interdependent network of information technology infrastructures, including the Internet, telecommunications networks, computer systems, and embedded processors and controllers".[54] By contrast, Russia and China regard cyberspace as an integrated part of information space, where human cognitive processes interact with all kinds of information. Therefore, cyber security should not be separated from information security that deals with information systems as well as human minds.[55] It should also be noted that even within the West, definitions of cyber security might still vary. For example, while the UK's cyber security strategy "places the logical layer (of cyberspace) at its center", the German counterpart adopts a narrow focus on "the virtual space of all IT systems linked at data level on a global scale".[56]

The unnerving implication is that these divergent national perspectives on cyber security may get entangled with political contention at the international level, which could in turn inhibit conceptual harmonization (academic and diplomatic alike) across different settings.[57] On this score, scholars from the US and Russia have engaged in a track-two effort to clarify cyber-security-related terminology and build a common perceptual foundation.[58] However, the outcome so far is not as promising as it aims. Giles and Hagestad critically pointed out that "the agreed definitions in each language did not actually match up with each other, leaving each side under the impression that consensus had been achieved but in fact remaining as far apart as ever".[59]

With regard to international organizations, the issue of cyber security has been on the agenda of the UN's General Assembly (both the First and the Second Committee) as early as 1998. But none of the resolutions approved as the result of these discussions offered clear definition of cyber security.[60] By contrast, the International Telecommunications Union (ITU) issued in 2008 an "Overview of Cybersecurity". It conceptualized cyber security as the combination of instruments, policies, norms, practices, institutions and technologies "that can be used to protect the cyber environment and

---

[53] James A. Lewis, "Cybersecurity and cyberwarfare: assessment of national doctrine and organization," in *UNIDIR: The Cyber Index: International Security Trends and Realities* (New York: United Nations, 2013).
[54] U.S. Department of Defense, *Department of Defense Dictionary of Military and Associated Terms* (2010): http://www.dtic.mil/doctrine/new_pubs/jp1_02.pdf.
[55] Keir Giles and William Hagestad II, "Divided by a Common Language: Cyber Definitions in Chinese, Russian and English," in *5th International Conference on Cyber Conflict*, ed. K. Podins, J. Stinissen, and M. Maybaum (Tallinn: NATO CCD COE Publications, 2013) https://ccdcoe.org/cycon/2013/proceedings/d3r1s1_giles.pdf
[56] Even and Siman-Tov, "Cyber Warfare," 12.
[57] Alexander Klimburg, "The Internet Yalta," *Center for a New American Security Commentary* (2013): http://www.cnas.org/sites/default/files/publications-pdf/CNAS_WCIT_commentary%20corrected%20%2803.27.13%29.pdf
[58] James B. Godwin III, Andrey Kulpin, Karl Frederick Rauscher, and Valery Yaschenko, eds. 2011. *Russia-U.S. Bilateral on Cybersecurity – Critical Terminology Foundations 2*. New York: East West Institute and the Information Security Institute of Moscow State University. http://www.iisi.msu.ru/UserFiles/File/Terminology%20IISI%20EWI/Russia-U%20S%20%20bilateral%20on%20terminology%202.pdf
[59] Giles and Hagestad, "Divided by a Common".
[60] Roxana Radu, "Power Technology and Powerful Technologies – Global Governmentality and Security in the Cyberspace," in *Cyberspace and International Relations: Theory, Prospects and Challenges*, ed. Jan-Frederik Kremer and Benedikt Müller (Switzerland: Springer, 2013).

Electronic copy available at: https://ssrn.com/abstract=2734336

organization and user's assets".[61] In addition to its ambiguous wording, this definition could be too inclusive to maintain any operational value. In fact, both the absence and the ambiguity of cyber security concepts in the above-mentioned documentation have probably reflected the politicization of framing cyber security within the international society.

3.4 Cyber Security as a Social Construct

Although the issue of cyber security has become a hot topic in security studies, discussions above demonstrate that a consensus has not been reached on precise meanings of relevant terms. It has been argued that current conceptualizations of cyber security are excessively broad and obscure in terms of the targets of cyber threats and the threats per se.[62] The conceptual basis of cyber security is further influenced by global political dynamics, since the framing of cyberspace and security problems has direct implications for the principles and institutions of global governance architecture.[63]

This point suggests the importance of the way in which security is constructed by socially interactive perceptions and debates. In this sense, security should be understood not only as an objective condition, but also as an intersubjective product of social construction.[64] Instead of focusing on the material aspects that constitute security, the constructive approach, especially the securitization theory, examines the process that specific "securitizing actors" effectively frame and present a security threat to their audience.[65] Meanwhile, the trajectory of that process is not randomly determined. Rather, different security sectors may involve particular threat agenda and feature distinct patterns of securitization.

Against this backdrop, the framework of securitization theory also sheds light on the discursive (intersubjective) dynamic that constructs cyber security. Accordingly, a number of studies have examined the internal mechanisms that shape cyber threat images, the alarming policy implications due to exaggerated cyber threat rhetoric, as well as perceptual foundations for international cyber security cooperation.[66] Although the primary objective of these studies is not to build a coherent definition for cyber security, they greatly contribute to our understanding of cyber security concept in at least two aspects. Firstly, they highlight the fact that discussions on cyber security are embedded in a web of threat discourse. Distinct strains of discourse can be identified by different actors who hold particular perspectives on cyber security and different models of reasoning used to portray and project cyber threats in particular manners. For instance, actors from a technical background may be more likely to depict cyber security problems as incidents stemming from the internal complexity of

[61] International Telecommunication Union, *Overview of Cybersecurity RecommendationX.1205*, https://www.itu.int/rec/T-REC-X.1205-200804-I.
[62] Dunn Cavelty, "Cyber-Terror-Looming Threat," 28.
[63] David Drissel, "Internet Governance in a Multipolar World: Challenging American Hegemony," *Cambridge Review of International Affairs* 19 (2006): 105-120; Klimburg, "The Internet Yalta".
[64] Michael C. Williams, "Words, Images, Enemies: Securitization and International Politics," *International Studies Quarterly* 47 (2003): 513.
[65] Buzan et al., "Security: A New Framework".
[66] Ronald Deibert, "Circuits of Power: Security in the Internet Environment," in *Information Technologies and Global Politics: The Changing Scope of Power and Governance*, ed. J.P. Singh and james N. Rosenau (New York: Suny Press, 2002), 115-142; Dunn Cavelty, "Cyber-Terror-Looming Threat"; Hansen and Nissenbaum, "Digital Disaster"; Betz and Stevens, "Analogical reasoning"; Dunn Cavelty, "From Cyber-Bombs"; Jerry Brito and Tate Watkins, "Loving the Cyber Bomb? The Dangers of Threat Inflation in Cybersecurity Policy," *Harvard National Security Journal* 3 (2011): 39-84; Sean Lawson, "Beyond Cyber-Doom: Assessing the Limits of Hypothetical Scenarios in the Framing of Cyber-Threats," *Journal of Information Technology & Politics* 10 (2013): 86-103; Nicholas Thomas, "Cyber Security"; Agnes Kasper, "The Fragmented Securitization of Cyber Threats," in *Regulating eTechnologies in the European Union: Normative Realtities and Trends*, ed. Tanel Kerikmäe (Switzerland: Springer, 2014), 157-187.

Electronic copy available at: https://ssrn.com/abstract=2734336

networked systems, thus implicating actions that would de-politicize security issues.[67] In contrast, strategic discourse may pay much attention to, and articulate on, unforeseen risks that could lead to political instability and even a cyber catastrophe. Due to the existence of "multi-discursivity" and competing threat images of cyber security, it would be rather difficult to achieve a precise, parsimonious and undisputable concept for all cyber stakeholders.[68] But, it would be also important to find a way to bridge the gap among divergent discourses and practices, and build a knowledge platform where discourses and conceptualizations of cyber security could converge.

This leads to the second aspect: studies on cyber securitization can be seen as a collective effort to systematically explore and establish the linkages among actors, targets and threats of cyber security. The multiple pathways to, and outcomes of, cyber threat representations, identified by securitization framework, have undoubtedly enhanced our understanding of the complex reality of cyber security. Nonetheless, the restricted focus of securitization studies on speech-acts means that other important elements of cyber security, such as instruments and motivations of cyber attacks, and specific context of cyber threats, may not be adequately addressed. This, again, necessitates an even more systematic and comprehensive approach to understand cyber security.

3.5 Bridging Diverse Discourses: From Taxonomy to Ontology

The conceptual underpinning of cyber security, as discussed above, is constructed by different discourses and approaches. But several observations can be made in regard to the common features of these studies.

To begin with, it is noteworthy that cyber security represents a collection of constantly changing phenomena. In this sense, a strictly defined cyber security concept may risk over-simplification and being static, especially given that information technologies are evolving dramatically. Lawson has remarked on this difficult and even paradoxical task "to acknowledge their (cyber threats) complexity and to work toward the clearest, most precise definitions possible, even when absolute clarity and precision are unattainable".[69]

Secondly, cyber security issues are found across different domains and penetrate different dimensions of human security. This indicates a holistic approach that can best illustrate the almost ubiquitous character of cyber in human activities. Efforts to conceptualize cyber security should thus encompass a wide spectrum of attributes rather than center on any single indicator of them.

Moreover, the relational aspect of cyber security should be taken into account in any conceptual framework. Unilateral investment in cyber security is often inadequate in enhancing the totality of security.[70] And actors, issues and systems in and through cyberspace become increasingly inter-dependent and intertwined that their connections could be as important as their properties. As a result, methods need to be identified that allow for simultaneously the demonstration of cyber security

[67] Dunn Cavelty, "From Cyber-Bombs."
[68] Hansen and Nissenbaum, "Digital Disaster," 1163.
[69] Lawson, "Beyond Cyber-Doom."
[70] Xingan Li, "Cybersecurity as a relative concept," *Information & Security: An International Journal* 18 (2006): 11-24.

Electronic copy available at: https://ssrn.com/abstract=2734336

attributes and the relationship among them.

In response to this need, some studies have attempted to establish organized formal models to better present the dynamic interactions within cyber security issues. On this score, a number of taxonomies have been built to classify cyber threats and attacks in a systemic way.[71] These models adopt different combinations of cyber threat attributes (categories), mostly including attackers, tools, actions, objectives, impacts, and defensive methods. This approach enables security practitioners to analyze patterns of threat behavior and linkages among different aspects of security incidents. For instance, when datasets are input into the proposed models, it is possible, and would be valuable, to locate a particular actor or a specific attack instrument, and identify all the security events associated with that actor/tool.[72] It contributes to revealing commonalities and regularities among cyber threats. However, there are still weaknesses firstly in that most studies in this regard focus on technical cyber attacks, which represent a narrow conceptualization that does not necessarily cover the full spectrum of cyber security.

The problem exists, probably because the proposed taxonomies are pragmatically designed to provide guidance for governmental (and organizational) defensive doctrines or strategies. Moreover, as Applegate and Stavrou acknowledged, taxonomy models are often bound to hierarchical categorizations, which may be incapable of capturing all possible relationships and mechanisms among different attributes.[73]

An ontological approach suggested by them, meanwhile, may alleviate or overcome both deficiencies mentioned above. Defined as an "explicit specification of conceptualization", ontology is often used as a means to facilitate knowledge sharing and reusability.[74] Using Web Ontology Language (OWL), it enables formalized representations of categories, attributes and relations involved in a specific domain. More importantly, it becomes possible to bridge the diversified meanings and expressions of a referent object, thus providing a common platform for different discourses. Nonetheless, current efforts to construct ontologies of cyber security are mainly made by technical communities that intend to understand malware and malicious activities more thoroughly.[75] They do not necessarily facilitate collaboration and knowledge-exchange with political and strategic communities concerned about cyber conflicts or political challenges in general.

In fact, a review on information security ontologies has remarked that a complete security ontology has not been developed that can provide "reusability, communication and knowledge

---

[71] John D. Howard, "An Analysis of Security Incidents on the Internet 1989-1995," PhD diss., (Carnegie Mellon University, 1997); Simon Hansman and Ray Hunt, "A taxonomy of network and computer attacks," *Computers & Security* 24 (2004): 31-43; Chris Simmons, Charles Ellis, Sajjan Shiva, Dipankar Dasgupta, and Qishi Wu, "AVOIDIT: A Cyber Attack Taxonomy," *Technical Report CS-09-003 University of Memphis* (2009): http://issrl.cs.memphis.edu/files/papers/CyberAttackTaxonomy_IEEE_Mag.pdf; Scott Applegate and Angelos Stavrou, "Towards a Cyber Conflict Taxonomy," presented at the 5th International Conference on Cyber Conflict, Tallin (2013); Kremer and Müller, "SAM".

[72] Applegate and Stavrou, "Towards a Cyber".

[73] Applegate and Stavrou, "Towards a Cyber".

[74] Thomas Gruber, "Toward principles for the design of ontologies used for knowledge sharing," *International Journal of Human-Computer Studies* 43 (1993): 907-928.

[75] Takeshi Takahashi, , Youki Kadobayashi, and Hiroyuki Fujiwara, "Ontological Approach toward Cybersecurity in Cloud Computing," in *Proceedings of the 3rd international conference on Security of Information and Networks,* ed. Frederick T. Sheldon, Stacy Prowell, Robert K. Abercrombie, and Axel Krings (2010): 100-109; Leo Obrsta, Penny Chase, and Richard Markeloff., "Developing an Ontology of the Cyber Security Domain, ed.ed. Paulo C. G. Costa and Kathryn B. Laskey, *Proceedings of Seventh International Conference on Semantic Technologies for Intelligence, Defense, and Security (STIDS)*, (2012): 49-56.

Electronic copy available at: https://ssrn.com/abstract=2734336

sharing".[76] To achieve this objective, development of cyber security knowledge models should not be confined to any single community and, instead, serve as an enabling factor that brings together divergent cyber security discourses. For example, the Global System for Sustainable Development (GSSD) has been constructed by researchers in MIT, which offers an interactive knowledge-networking platform that diversified technologies, instruments, ideas and policies related to sustainable development can easily communicate.[77] With similar logic, the Cyber System for Strategic Decisions (CSSD) is currently under construction that would allow for comprehensive knowledge sharing and generation in the cyber domain.

Cyber security has become an influential aspect of international security studies in the twenty-first century. But our review on the conceptual underpinning of cyber security suggests that different discourses coexist and have divergent views on what constitutes cyber security and threats. Organized formal models, such as taxonomy and ontology, represent a systematic way of conceptualization that has potential for bridging multi-discursivity in current cyber security studies. How to fully engage and include the heterogeneous stakeholders of cyber security into this process, meanwhile, remains an important question for future research.

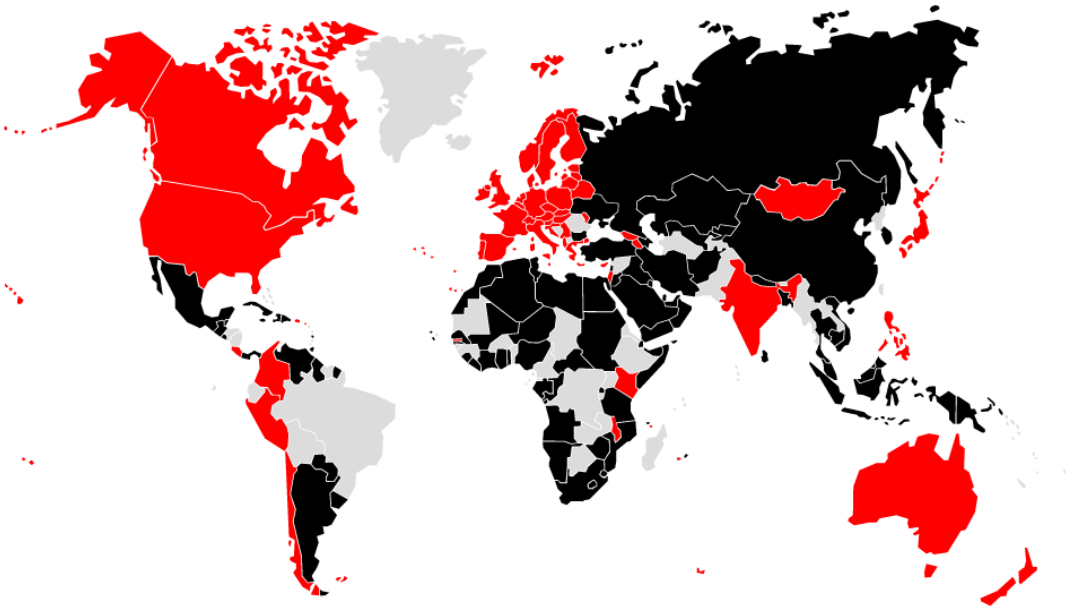


Figure 3.3
Map depicting Final Signatories at WCIT 2012
(countries in black are signatories of the Final Acts, while red indicates non-signatories)

[76] Carlos Blanco, Joaquin Lasheras, Rafael Valencia-Garcia, Eduardo Fernandez-Medina, Ambrosio Toval, and Mario Piattini, "A Systematic Review and Comparison of Security Ontologies," presented at *The Third International Conference on Availability, Reliability and Security*, Barcelona, Spain,, (2008): March 4-7,
[77] Nazli Choucri, "Mapping Sustainability," MIT Global System for Sustainable Development Working Paper (2003).

Electronic copy available at: https://ssrn.com/abstract=2734336

References

Applegate, Scott. 2013. The Dawn of Kinetic Cyber. Presented at the 5th International Conference on Cyber Conflict, Tallinn, June 4-7, 2013.

Applegate, Scott and Angelos Stavrou. 2013. Towards a Cyber Conflict Taxonomy. Presented at the 5th International Conference on Cyber Conflict, Tallinn, June 4-7, 2013.

Betz, David J. and Tim Stevens. 2013. Analogical reasoning and cyber security. *Security Dialogue* 44 (April): 147-164.

Blanco, Carlos, Joaquin Lasheras, Rafael Valencia-Garcia, Eduardo Fernandez-Medina, Ambrosio Toval, and Mario Piattini. 2008. A Systematic Review and Comparison of Security Ontologies. Presented at The Third International Conference on Availability, Reliability and Security, Barcelona, Spain, March 4-7, 2008.

Brito, Jerry and Tate Watkins. 2011. Loving the Cyber Bomb? The Dangers of Threat Inflation in Cybersecurity Policy. *Harvard National Security Journal* 3 (1): 39-84.

Brown, Gary D. and Owen W. Tullos. 2012. On the Spectrum of Cyberspace Operations. *Small Wars Journal*. (December 11): http://smallwarsjournal.com/print/13595.

Buzan, Barry, Charles Jones, and Richard Little. 1993. *The Logic of Anarchy: Neorealism to Structural Realism.* New York: Columbia University Press.

Buzan, Barry, Ole Wæver, and Jaap de Wilde. 1998. *Security: A New Framework for Analysis*. Boulder, CO: Lynne Rienner Publishers.

Buzan, Barry and Lene Hansen. 2009. *The Evolution of International Security Studies*. Cambridge: Cambridge University Press.

Chandrashekar, Jaideep, Steve Orrin, Carl Livadas, and Eve Schooler. 2009. The Dark Cloud: Understanding and Defending against Botnets and Stealthy Malware. *Intel Technology Journal* 13 (August): 130-147.

Choucri, Nazli. 2003. "Mapping Sustainability". MIT Global System for Sustainable Development Working Paper.

Choucri, Nazli. 2012. *Cyberpolitics in International Relations*. Cambridge, MA: The MIT Press.

Choucri, Nazli and David Clark. 2011. Cyberspace and International Relations: Toward an Integrated System. Paper presented at Massachusetts Institute of Technology, Cambridge, Massachusetts, August 25, 2011.

Electronic copy available at: https://ssrn.com/abstract=2734336

Choucri, Nazli, Stuart Madnick, and Jeremy Ferwerda. 2013. Institutions for Cyber Security: International Responses and Global Imperatives. *Information Technology for Development*. DOI: 10.1080/02681102.2013.836699.

Cohen, Julie E. 2007. Cyberspace as/and Space. *Columbia Law Review* 107 (January): 210-256.

Cornish, Paul, Rex Hughes, and David Livingstone. 2009. *Cyberspace and the National Security of the United Kingdom: Threats and Responses*. London: Chatham House.

Deibert, Ronald. 2002. "Circuits of Power: Security in the Internet Environment." In J.P. Singh and James N. Rosenau, eds., *Information Technologies and Global Politics: The Changing Scope of Power and Governance*, 115-142, New York: Suny Press.

Deibert, Ronald and Rafal Rohozinski. 2010. Risking Security: The Policies and Paradoxes of Cyberspace Security. *International Political Sociology* 4 (March): 15-32.

Deibert, Ronald. 2012. The Growing Dark Side of Cyberspace (… and What To Do About It). *Penn State Journal of Law & International Affairs* 1 (November): 260-274.

DeNardis, Laura. 2009. *Protocol Politics: The globalization of Internet governance*. Cambridge, MA: The MIT Press.

Drezner, Daniel. 2004. The Global Governance of the Internet: Bringing the State Back In. *Political Science Quarterly* 119 (February): 477-498.

Drissel, David. 2006. Internet Governance in a Multipolar World: Challenging American Hegemony. *Cambridge Review of International Affairs* 19 (1): 105-120.

Dunn Cavelty, Myriam. 2007. Cyber-Terror–Looming Threat or Phantom Menace? The Framing of the US Cyber-Threat Debate. *Journal of Information Technology and Politics* 1 (4): 19-36

Dunn Cavelty, Myriam. 2008. *Cyber-Security and Threat Politics: US Efforts to Secure the Information Age*. New York: Routledge.

Dunn Cavelty, Myriam. 2013. From Cyber-Bombs to Political Fallout: Threat Representations with an Impact in the Cyber-Security Discourse. *International Studies Review* 15 (March): 105-122.

Eriksson, Johan and Giampiero Giacomello. 2006. The Information Revolution, Security, and International Relations: (IR) Relevant Theory? *International Political Science Review* 27 (July): 221-244.

Even, Shmuel and David Siman-Tov. 2012. Cyber Warfare: Concepts and Strategic Trends. *The Institute for National Security Studies Memorandum* 117.

Electronic copy available at: https://ssrn.com/abstract=2734336

http://www.inss.org.il/upload/(FILE)1337837176.pdf

Ewan, Pauline. 2007. Deepening the Human Security Debate: Beyond the Politics of Conceptual Clarification. *Politics* 27 (October): 182-189.

Farwell, James P. and Rafal Rohozinski. 2011. Stuxnet and the Future of Cyber War. *Survival* 53 (February): 23–40.

Gibson, William. 1984. *Neuromancer*. New York: Ace Books.

Giles, Keir. 2012. Russia's Public Stance on Cyberspace Issues. In C. Czosseck, R. Ottis, K. Ziolkowski eds., 4th International Conference on Cyber Conflict, 63-77, Tallinn: NATO CCD COE Publications.

Giles, Keir and William Hagestad II. 2013. Divided by a Common Language: Cyber Definitions in Chinese, Russian and English. In K. Podins, J. Stinissen, and M. Maybaum eds., *5th International Conference on Cyber Conflict*, Tallinn: NATO CCD COE Publications. https://ccdcoe.org/cycon/2013/proceedings/d3r1s1_giles.pdf

Goldsmith, Jack L. and Tim Wu. 2006. *Who Controls the Internet?: Illusions of a Borderless World*. Oxford: Oxford University Press.

Godwin III, James B., Andrey Kulpin Karl Frederick Rauscher, and Valery Yaschenko, eds. 2011. *Russia-U.S. Bilateral on Cybersecurity – Critical Terminology Foundations 2*. New York: East West Institute and the Information Security Institute of Moscow State University. http://www.iisi.msu.ru/UserFiles/File/Terminology%20IISI%20EWI/Russia-U%20S%20%20bilateral%20on%20terminology%202.pdf

Graham, Mark. 2013. Geography/Internet: ethereal alternate dimensions of cyberspace or grounded augmented realities? *The Geographical Journal* 179 (2): 177-182.

Gregory, M.A. and David Glance. 2013. *Security and the Networked Society*. Switzerland: Springer.

Gruber, Thomas. 1995. Toward principles for the design of ontologies used for knowledge sharing. *International Journal of Human-Computer Studies* 43 (November/December): 907-928.

Guttman, Barbara and Edward Roback. 1995. *An Introduction to Computer Security: The NIST Handbook*. Gaithersburg, MD: U.S. Department of Commerce.

Hansen, Lene and Helen Nissenbaum. 2009. Digital Disaster, Cyber Security, and the Copenhagen School. *International Studies Quarterly* 53 (December): 1155-1175.

Hansman, Simon and Ray Hunt. 2004. A taxonomy of network and computer attacks. *Computers &*

Electronic copy available at: https://ssrn.com/abstract=2734336

Security 24 (February): 31-43.

Hartmann, Kim and Christoph Steup. 2013. The Vulnerability of UAVs to Cyber Attacks - An Approach to the Risk Assessment. In K. Podins, J. Stinissen, and M. Maybaum eds., *5th International Conference on Cyber Conflict*, Tallinn: NATO CCD COE Publications. https://ccdcoe.org/cycon/2013/proceedings/d3r2s2_hartmann.pdf

Healey, Jason and Karl Grindal, eds. 2013. *A Fierce Domain: Conflict in Cyberspace, 1986 to 2012*. Vienna, VA: Cyber Conflict Studies Association.

Howard, John D. 1997. "An Analysis of Security Incidents on the Internet 1989-1995." PhD diss., Carnegie Mellon University.

Hughes, Christopher R. 2010. Google and the Great Firewall. *Survival* 52 (2): 19–26.

International Telecommunication Union. 2008. Overview of Cybersecurity. Recommendation X.1205. https://www.itu.int/rec/T-REC-X.1205-200804-I.

Karim, Md E. and Vir V. Phoha. 2013. Cyber-physical Systems Security. In *Applied Cyber-Physical Systems*, ed. Sang C. Suh, U. John Tanik, John N. Carbone, and Abdullah Eroglu, 75-83. Switzerland: Springer.

Kasper, Agnes. 2014. The Fragmented Securitization of Cyber Threats. In *Regulating eTechnologies in the European Union: Normative Realities and Trends*, ed. Tanel Kerikmäe, 157-187. Switzerland: Springer.

King, Gary and Christopher Murray. 2001. Rethinking Human Security. *Political Science Quarterly* 116 (4): 585-610.

Klimburg, Alexander. 2013. The Internet Yalta. *Center for a New American Security Commentary*. (February): http://www.cnas.org/sites/default/files/publications-pdf/CNAS_WCIT_commentary%20corrected%20%2803.27.13%29.pdf

Knapp, Eric and Joel T. Langill. 2011. *Industrial Network Security: Securing Critical Infrastructure Networks for Smart Grid, SCADA, and Other Industrial Control Systems*. Rockland, MD: Syngress Publishing.

Kremer, Jan-Frederik and Benedikt Müller. 2014. SAM: A Framework to Understand Emerging Challenges to States in an Interconnected World. In *Cyberspace and International Relations: Theory, Prospects and Challenges*, ed. Jan-Frederik and Benedikt Müller, 41-58. Switzerland: Springer.

Lawson, Sean. 2013. Beyond Cyber-Doom: Assessing the Limits of Hypothetical Scenarios in the Framing of Cyber-Threats. *Journal of Information Technology & Politics* 10 (February): 86-103.

Electronic copy available at: https://ssrn.com/abstract=2734336

Lewis, James A. 2013. Cybersecurity and cyberwarfare: assessment of national doctrine and organization. In *UNIDIR: The Cyber Index: International Security Trends and Realities*. New York: United Nations.

Lewis, James A. 2014. Cyber Threat and Response: Combating Advanced Attacks and Cyber Espionage. *Center for Strategic & International Studies Report* (March).

Li, Xingan. 2006. Cybersecurity as a relative concept. *Information & Security: An International Journal* 18 (January): 11-24.

Libicki, Martin C. 2007. *Conquest in Cyberspace: National Security and Information Warfare*. Cambridge: Cambridge University Press.

Lynn III, William J. 2010. Defending a New Domain: The Pentagon's Cyberstrategy. *Foreign Affairs* 89 (September/October): 97-108.

Mandiant. 2013. APT1: Exposing One of China's Cyber Espionage Units. http://intelreport.mandiant.com/Mandiant_APT1_Report.pdf.

Mathiason, John. 2008. *Internet Governance: The New Frontier of Global Institutions*. London: Routledge.

Mueller, Milton. 2010. *Networks and States: The Global Politics of Internet Governance*. Cambridge, MA: The MIT Press.

Mueller, Milton, Andreas Schmidt, and Brenden Kuerbis. 2013. Internet Security and Networked Governance in International Relations. *International Studies Review* 15 (March): 86-104.

National Academy of Sciences. 1991. *Computers at risk: Safe computing in the information age*. Washington, D.C.: National Academy Press.

Nye, Joseph S. 2010. Cyber Power. Paper, Belfer Center for Science and International Affairs, Harvard Kennedy School (May).

Nye, Joseph S. 2011. Nuclear Lessons for Cyber Security? *Strategic Studies Quarterly* 5 (Winter): 18-38.

Obrsta, Leo, Penny Chase, and Richard Markeloff. 2012. Developing an Ontology of the Cyber Security Domain. In ed. Paulo C. G. Costa and Kathryn B. Laskey, *Proceedings of Seventh International Conference on Semantic Technologies for Intelligence, Defense, and Security (STIDS)*, 49-56.

Radu, Roxana. 2014. Power Technology and Powerful Technologies - Global Governmentality and Security in the Cyberspace. In *Cyberspace and International Relations: Theory, Prospects and*

Electronic copy available at: https://ssrn.com/abstract=2734336

Challenges, ed. Jan-Frederik Kremer and Benedikt Müller, 3-21. Switzerland: Springer.

Reveron, Derek S. 2012. An Introduction to National Security and Cyberspace. In *Cyberspace and National Security: Threats, Opportunities, and Power in a Virtual World*, ed. Derek S. Reveron, 3-20. Washington, D.C.: Georgetown University Press.

Rid, Thomas. 2013. *Cyber War Will Not Take Place*. Oxford: Oxford University Press.

Sartori, Giovanni. 1970. Concept Misformation in Comparative Politics. *American Political Science Review* 4 (1970): 1033-1053.

Simmons, Chris, Charles Ellis, Sajjan Shiva, Dipankar Dasgupta, and Qishi Wu. 2009. AVOIDIT: A Cyber Attack Taxonomy. Technical Report CS-09-003, University of Memphis. http://issrl.cs.memphis.edu/files/papers/CyberAttackTaxonomy_IEEE_Mag.pdf.

Stern, Maria and Joakim Öjendal. 2010. Mapping the Security–Development Nexus: Conflict, Complexity, Cacophony, Convergence? *Security Dialogue* 41 (February): 5-29.

Symantec. 2014. Internet Security Threat Report 19 (April): http://www.symantec.com/about/news/resources/press_kits/detail.jsp?pkid=istr-19

Takahashi, Takeshi, Youki Kadobayashi, and Hiroyuki Fujiwara. 2010. Ontological Approach toward Cybersecurity in Cloud Computing. In ed. Frederick T. Sheldon, Stacy Prowell, Robert K. Abercrombie, and Axel Krings, *Proceedings of the 3rd international Conference on Security of Information and Networks*, 100-109.

Thomas, Caroline. 2001. Global Governance, Development and Human Security: Exploring the Links. *Third World Quarterly* 22 (April): 159-175

Thomas, Nicholas. 2009. Cyber Security in East Asia: Governing Anarchy. *Asian Security* 5 (1): 3-23.

Tilly, Charles. 2003. *The Politics of Collective Violence*. Cambridge: Cambridge University Press.

U.S. Department of Defense. 2010. *Department of Defense Dictionary of Military and Associated Term*s. http://www.dtic.mil/doctrine/new_pubs/jp1_02.pdf.

Ullman, Richard H. 1983. Redefining Security. *International Security* 8 (Summer): 129-153.

United Nations Development Programme. 1994. *Human Development Report*. New York: Oxford University Press.

Valeriano, Brandon and Ryan C. Maness. 2014. The dynamics of cyber conflict between rival antagonists, 2001-11. *Journal of Peace Research* 51 (May): 347-360.

Electronic copy available at: https://ssrn.com/abstract=2734336

Williams, Michael C. 2003. Words, Images, Enemies: Securitization and International Politics. *International Studies Quarterly* 47 (December): 511-531.

Wilson, Kelce S. and Muge Ayse Kiy. 2014. Some Fundamental Cybersecurity Concepts. *IEEE Access* 2 (February): 116-124.

Wolfers, Arnold. 1952. "National Security" as an Ambiguous Symbol. *Political Science Quarterly* 67 (December): 481-502.

Zedner, Lucia. 2009. *Security*. London: Routledge.

Electronic copy available at: https://ssrn.com/abstract=2734336

4. Cyberspace as the Domain of Content

Lyla Fischer

On the Internet, content is king. This silicon-valley proverb has helped many technologists focus their start-ups on high-impact areas, and might prove useful to policymakers deciding where to focus their efforts on behalf of their stakeholders.

While it is possible to consider cyberspace in terms of its mechanics (eg. networks, sensors, storage devices, algorithms), the constant progress produced by high technology creates a fluidity and complexity that can make it prohibitively difficult for policymakers to know how to influence its activities and hold experts accountable for specific, verifiable objectives.

This paper aims to differentiate between the ends and means of cyberspace so that policymakers can focus on the ends and experts can specialize in the means.

The first step is to define cyberspace as a whole in the same way programs within it are defined: specifying inputs, actions on those inputs, and outputs. Within cyberspace, every input is a bit of information or piece of content, actions on inputs are accomplished using modern technology, and the resulting content outputs an effect on the real world. The longevity of any particular policy can be estimated by its ability to avoid dependence on specific technological implementations.

4.1 Effects of Information and Knowledge

Information and knowledge encoded as digital content is of interest because of effects in the real world. Note that while modern technology can reduce the amount of marginal human intervention for content to have an effect, information and knowledge often produce effects without modern technology. Listed here are common effects that information and knowledge can have.

4.1.1 Entertainment:

Some knowledge is treated like a consumer good. Everyday people enjoy stories, songs, pictures, plays, and games with little regard to usefulness outside of the pleasure that they bring to daily life. Artistic entertainment does not necessarily require modern technology; songs have existed much longer than the microphone. However, people have been able to use modern technology to transform traditional art forms and create new forms of expression that bring joy into people's lives.

Physical Systems:

Knowledge that has historically been trained into humans as skills can be encoded digitally to send electric force through motors. Those motors can move power equipment, control the elevators and climate in buildings, optimize the fuel efficiency in cars, direct current through the power grid, and even automate complex tasks like the flight systems on airplanes.

Electronic copy available at: https://ssrn.com/abstract=2734336

4.1.2 Technology development:

One of the most concentrated forms of recorded knowledge is a specification or design of high technology. The designs themselves do not produce effects until they have been translated into physical objects through manufacturing and assembly. However, the design is still an extremely valuable asset, and a critical part of the supply chain for those goods.

Note that source code can be considered a subcategory of design. Source code cannot produce effects until it is compiled and deployed on physical computers.

4.1.3 Decision-making:

One of the most familiar and most important effects of knowledge and information is its influence on decision-making. Decision-makers have demonstrated need for high quality knowledge, information, and understanding long before technology developed to its current state, but only in the last century have decision-makers have been unable to personally manage and verify their entire informational supply chain.

4.1.4 Plans:

Information is also quite valuable to non-decision-makers who need to understand the actions that they need to take according to a coordinated plan. A plan by itself cannot produce results without being distributed, contextualized, and executed.

4.2 Capabilities of Modern Technology

Modern technology has four major capabilities that have transformed the effects of information and knowledge.

4.2.1 Speed and Distance of Communication (Networks):

The Morse Telegraph System finished replacing the Pony Express in 1861. That technology eventually became a phone system, and then the hardware basis for the Internet. Electronic communication systems allowed people to conduct commerce, diplomacy, and personal connection at a pace decoupled from the transportation of people and packages. New technological developments continually allow us to transmit more files, larger files, and have those files arrive sooner.

4.2.2 Logic, Patterns, and Simulation (Computation):

Alan Turing built the first non-theoretical computational device in 1941 in order to transform intercepted German communications into a format that allied forces could read. Since then, we have been able to automatically alter information into formats that fit our needs with increasing sophistication. This alteration often requires humans to identify and program mathematical trends and patterns into computers. Computers are useful for quickly translating large numbers of inputs or simulating the results of large numbers of guesses. As technology develops, we can translate more inputs and simulate more guesses in the same amount of time, while making fewer mathematical

Electronic copy available at: https://ssrn.com/abstract=2734336

simplifications.

4.2.3 Recording and Records (Sensors, Storage):

Bing Crosby popularized the audio recording in 1947 by pioneering the pre-recorded radio show, allowing him to invest highly in production values and use the resulting shows for multiple broadcasts. The work he did while pairing information storage with electronic distribution earned him several stars on the Hollywood Walk of Fame. Since then, technology has made it easier and easier to collect and store larger and larger amounts of information, and has made it easier and faster to alter that stored content using automatic logic.

4.2.4 Human-Computer Interaction (HCI):

The power of sophisticated tools is increasingly used by untrained non-experts because technology has gotten cheaper and easier to use. As desktop computers became affordable around 1983, spreadsheet application Lotus1-2-3 revolutionized small business record keeping and Apple Computer foraged into desktop publishing with What-You-See-Is-What-You-Get (WYSIWYG, pronounced wiss-ee-wig) interfaces. As technology continues to develop, we will see more technological capabilities used with less training and lower capital investment.

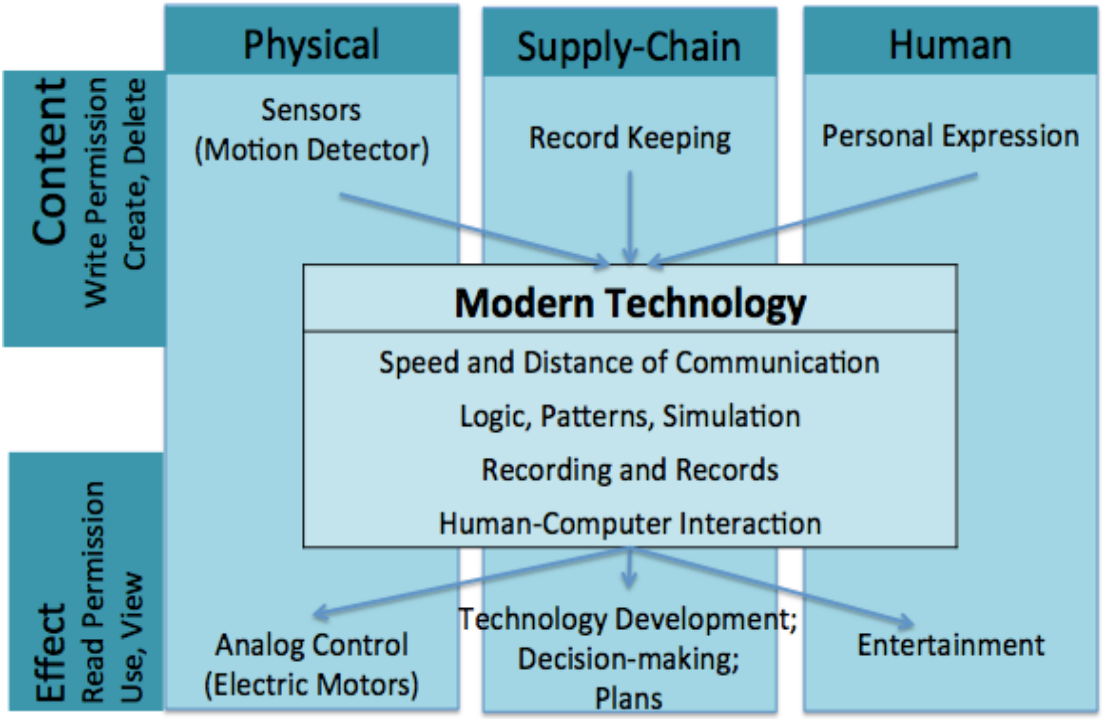


Figure 4.1
The informational domain has a set of capabilities that can take inputs and produce outputs.

4.3 Types of Content

We have outlined some of the major effects that information and knowledge can produce. We

Electronic copy available at: https://ssrn.com/abstract=2734336

have categorized the advances that modern technology has brought to how we can leverage information and knowledge. However, categorizing information and knowledge remains an underdeveloped area of understanding, in both theory and practice.

Some information is already well controlled because it contributes to important effects in well-known ways, even without the added sophistication of modern technology. Examples include financial records, business accounts, medical records, correspondence, and personal dairies as well as more processed knowledge such as reports, plans, and designs.

Advances of modern technology have allowed us to capture and process information in ways that have augmented the importance of certain assets beyond their historical levels. Without any human intervention, sensors can store facts about the physical world from which logical programs can draw valuable conclusions. Records and reports that used to propagate through paper and human memory are now automatically indexed and searched by metadata, keyword, or other pattern. Social interactions that used to be fleeting and isolated to geographic locations are now international and recorded in perpetuity. Many of these assets are both unregulated and undisputed because they were unable to produce outputs of interest before the application of modern technology.

That is no longer the case.

Policymakers need to understand the impact of information that was previously of minimal value so that they can prioritize and protect their interests from the effects that unclaimed or unprotected information or knowledge might produce for opposing interests.

While it is always better to have a deep understanding of everything one might ever encounter, significant policy guidelines can be produced using only the implications of four main modern technological capabilities. In order to illustrate technology policy using only this limited abstraction of modern technology, I will explain how the music industry was disrupted and how it recovered from the effect of internet-connected desktop computers.

4.4 Case Study: The Recording Industry and the Internet

With the rise of the World Wide Web in the 1990's, many middle class Americans purchased internet-connected desktop computers. Those purchases provided the technical ability for everyday people to upload and make available any information to which they had access.

4.4.1 Status quo:

One particularly interesting type of content is a music file. Before the rise of the internet, a distribution mechanism already existed for recorded music. Specifically, CDs were sold at stores. Common understanding was that after purchasing a CD, the owner could do whatever they wanted with that asset. They could play it at a party. They could lend it to a friend. They could make a mix-tape for their romantic interest. They *owned* the music.

Studios put a significant amount of investment into the development, curation, publicity, and

Electronic copy available at: https://ssrn.com/abstract=2734336

distribution of music. Studios recuperated that investment from sales made in stores, a well-enforced barrier of access for people to listen to and enjoy the results of a studio's investment.

4.4.2 The effect of technology:

This arrangement worked well until internet-connected personal computers allowed CD owners to give strangers copies of that CD at no cost to themselves. That is: minimally trained users were able to use a communication network to transfer copies of musical content over long distances.

Much of the technical complexity of that sharing ability was handled by yet another piece of technology: the user application called Napster. Most users did not know how a CD was read by a computer, how that computer stored the information read from a CD on a hard drive, how the computer was connected to the internet, how other computers could remotely request copies of content from a hard drive, how a computer could upload content from a hard drive to the internet, how a computer could copy content from the internet to a hard drive, or how content from a hard drive could be transformed into sound. Despite the common lack of knowledge of the mechanics of the music transfer, these activities were able to take place because Napster provided an interface that took care of significant portions of this complexity.

Finally, there was little ethical understanding around the usage of digital content. Most people who bought a CD were under the impression that it was perfectly acceptable to do anything within their power with the asset that they owned. They saw no difference between lending a CD to a friend, allowing that friend to make a copy of the CD, allowing that friend to download a copy of that CD from their computer, and allowing strangers to download a copy of that CD from their computer. Many people thought that if they bought music, and it was theirs to do with as they pleased.

The technological capabilities provided by the internet, desktop computers, and Napster, along with the ethical understanding of acceptable use of musical content after purchase, caused the music industry to temporarily lose the ability to charge money in order to derive enjoyment from their informational assets. It was cheaper and easier to download a song from Napster than to go to a store and purchase a CD.

4.4.3 The resolution:

The music industry was able to use existing legal precedent of copyright to establish that the common understanding of a user's rights after purchasing a CD was incorrect. Armed with that legal judgment, studios were able use legal authority to assert control over a particular piece of information that produced a specific desirable entertaining outcome. They used that authority to prosecute several users, but it soon became clear that the high costs associated with identification and prosecution of violators was prohibitive as long as violations requiring separate lawsuits were small scale. The music industry needed to find other methods of enforcing its control over its property.

The music industry won a key lawsuit against the creators of Napster, the user application that allowed people to violate copyright with minimal technical knowledge. It was not obvious that the

Electronic copy available at: https://ssrn.com/abstract=2734336

precedents associated with copyright would apply to Napster, but the trail of that specific case established the precedent that information services that allow people to share files with each other bear the legal responsibility for ensuring that people have the right to share those files with each other.

Prosecuting Napster did not solve all of the music industry's problems, because all of the technology that Napster was built on was still readily available. The internet was still free and open. Desktop computers were still in people's houses, providing cheap storage and computation. CDs were still distributed in formats that could be copied and stored on the hard drives of desktop computers. After shutting down Napster, other file-sharing services soon appeared to take Napster's place. There were few enough replacement services that it was possible to also prosecute them and shut them down. Compared to the number of people who used services like Napster, it was still much easier to enforce copyright only against the people who were capable of managing the complexity of putting together interfaces that made it **easy** to illegally download music.

As restrictions on downloading copyrighted music were increasingly enforced and practitioners were driven underground, accessing content illegally meant exposure to other illegal material. It just so happened that computer viruses were distributed on file-sharing sites under the disguise of desirable musical assets. Users who wanted the protection of the law from computer viruses had to abide by the law regarding copyright.

Finally, the music industry offered a legal alternative to file-sharing sites: iTunes. The iTunes software not only offered an online distribution mechanism that included purchasing, it also allowed the music industry to impose technological controls. It was more difficult to copy music stored on an iPod than it was to copy music stored on a CD, and that difficulty was intentionally intensified in various ways. iTunes did not include any ability for an end-user to send purchased music to friends. While untrained users lost a significant amount of control over music files, the iPod still allowed users to enjoy the output of the investment made by the recording studio. For many people, it became better to pay a small fee to legally download a song from iTunes than to understand and traverse an increasingly confusing and dangerous black market for free musical files.

4.4.5 Observations:

The fall of Napster and the rise of iTunes is the story of control over a specific type of content (music files) in order to control and charge for a specific effect (the enjoyment of musical performances). This control was eventually exerted though user-level applications, Napster and iTunes.

The music industry initially tried to apply a legal precedent that most naturally applied to a specific informational asset, but the fact that it was used by such a large set of disperse actors made enforcement difficult. In order to overcome practical implications of enforcement, that legal principle was translated to a smaller set of actors who organized large amounts of activity and who could be held accountable for the activity that it organized.

By focusing its prosecutorial efforts on a small number of specific players in a specific part of

Electronic copy available at: https://ssrn.com/abstract=2734336

the technological flow, the music industry was able to increase the expertise required to violate the law and to unbundle the acquisition of free musical material from other benefits law enforcement. They also decreased the cost and inconvenience of using a legal alternative so that there was less incentive to acquire expertise or brave danger.

As policymakers consider how different interests will be affected by modern technology, they will repeatedly come across the trend that technology makes information extremely mobile. Historically, it was possible to transfer an informational asset and trust that it would not be transferred further merely due to practical reasons, but technology is pushing those practicalities into irrelevance. The music industry discovered this fact with music files in the 90's, and was forced to adjust both its distribution mechanisms and its price point. Other forms of content are in the process of adjusting to this reality as well.

While applying methods of control to content that has changed in value, policymakers in non-musical fields are unlikely to face exactly the same set of constraints, incentives, costs, or competing interests that the music industry faced. Application of new policies will likely depend on different points in the technological flow where it is easiest to change the cost function of actors pursuing potentially competing interests. Policymakers will likely need to work with specialists to understand which costs will be easiest to adjust, and with other policymakers to understand the impact of potential policies on a wide variety of stakeholders.

Electronic copy available at: https://ssrn.com/abstract=2734336

5. DoD Perspective on Cyberspace

Glenn Voelz

The emergence of threats from "cyberspace" present new national security challenges for state actors, particularly technology-dependent nations whose political, economic and military powers are reliant upon information technology and networked computer systems. For these countries, including the U.S., the exercise of military power increasingly demands uninterrupted access to globally interconnected command and control systems, communications, guidance and navigation systems, intelligence-gathering platforms, and logistics networks. Additionally, sensitive intellectual property and defense-related information residing in the Defense Industrial Base is vulnerable to these new forms of attacks, as well as industrial infrastructure and economic assets. In 2013, the Director of National Intelligence identified cyber attacks as the number one strategic threat to the United States, placing it ahead of terrorism for the first time since the attacks of 9/11.[78] These threats have grown in complexity as a wider range of actors engage in such activities, including "profit-motivated criminals, ideologically motivated hackers or extremists and variously-capable nation-states like Russia, China, North Korea and Iran," according to recent testimony by the Director of National Intelligence.[79]

Analysts generally agree that the cyber domain presents a unique set of challenges for U.S. national security, specifically due to the fact that the cyber domain affords adversaries unprecedented reach, speed, and anonymity. Additionally, the cyber domain is generally considered to offer tactical advantage to the offense.[80] These characteristics have increased the ability of state and non-state actors to use distributed computer systems for the purposes of espionage, crime, terrorism, and even physical attacks as part of larger conventional military campaigns.

5.1 Developing a Taxonomy of Cyber:

As a relatively new national security concern, there remains significant debate over the basic matter of taxonomy, specifically how to define and categorize these threats. A clear understanding of what constitutes an attack within this domain is a necessary prerequisite for developing appropriate policies and response options. For the purpose of this discussion, the term *cyberwarfare* generally refers to state-on-state actions, equivalent to an armed attack or use of force in cyberspace that may trigger a military response with a proportional kinetic use of force.[81] Acts of *cyberterrorism* involve the "the premeditated use of disruptive activities, or the threat thereof, against computers and/or networks, with the intention to cause harm or further social, ideological, religious, political or similar objectives, or to intimidate any person in furtherance of such objectives." Distinct from these is the issue of *cybercrime*, involving "unauthorized network breaches and theft of intellectual property and other data; it can be financially motivated, and response is typically the jurisdiction of law enforcement agencies." *Cyberespionage* is also considered a distinct activity involving the theft of "classified or proprietary information used by governments or private corporations to gain a

[78] U.S. Department of Defense, *The Department of Defense Cyber Strategy* (Washington, DC: April 2015), 9.
[79] James R. Clapper, *Opening Statement to the Worldwide Threat Assessment Hearing*, Senate Armed Services Committee, February 26, 2015. http://www.dni.gov/index.php/newsroom/testimonies/209-congressional-testimonies-2015/1175-dni-clapper-opening-statement-on-the-worldwide-threat-assessment-before-the-senate-armed-services-committee
[80] For elaboration of these concepts see Dakota L. Wood and Heritage Foundation, *Index of U.S. Military Strength: Assessing America's Ability to Provide for the Common Defense* (Washington DC: Heritage Foundation, 2015), 74.
[81] For overview see Catherine A. Theohary and John W. Rollins, *Cyberwarfare and Cyberterrorism: In Brief* (Washington DC: Congressional Research Service, 2015), 1.

Electronic copy available at: https://ssrn.com/abstract=2734336

competitive strategic, security, financial, or political advantage."

Comparing Conventional Warfare versus Cyberwarfare[82]

	Conventional Warfare	Cyberwarfare
Political Context	Westphalian construct; conflicts waged by professional armies and state actors pursuing well-defined geo-political objectives. Grounded in conventional deterrence theories. Clear and well-established distinctions between warfare, terrorism, espionage and criminal behavior. Activities governed by established convention (law of war, Geneva, Hague, etc).	Extra-Westphalian; potentially involving both state and non-state actors pursuing financial, political or ideological causes, sometimes with ambiguous objectives. Uncertain rile for deterrence theories. Unclear distinctions between warfare, terrorism, espionage and criminal behavior. No clearly established norms for offensive cyber activities and use as a part of military campaigns.
Adversary Characteristics	Warfare waged by state armies and professional soldiers using doctrinal organized formations and functioning by depersonalized, bureaucratic logic. Adversaries are constrained by geographic space, logistics and industrial capacity.	Warfare waged by state as well as non-state entities. Some may use anonymity for operational advantage; use idiosyncratic tactics and organized around highly disaggregated networks. Adversaries are unconstrained by geography and distance. Power not directly linked to industrial capacity.
Operational Environment	Contested primarily in the conventional physical domains of war (land, sea, air, space) and waged in a contiguous linear battle-space; zone of conflict is defined by clear operational boundaries, fire and maneuver over geographic terrain. Conflict defined by measures conventional military power.	Contested primarily in the informational and cyber domain; spatially and temporally unbounded; defined by a merger of external and domestic security spheres of concern concerns. May include unconventional targets such as financial, infrastructure, private or pubic institutions.
Theories of War-Fighting	Influenced by tenets of maneuver warfare: mass, firepower, destruction of enemy forces and seizure of key terrain. Focus is on the operational level of war. Tactical advantage is to the Defense; however, cyber has also become a weapon of conventional warfare.	Influenced by technology theories and information warfare doctrines. Defined by unconventional approaches that do not align with traditional war-fighting theories. Tactical advantage is to the Offense.
Targeting Paradigm	Status-based targeting against legitimate military targets with focus on units, formations and equipment; Well-defined rules of engagement.	No clearly defined norms of targeting. Private and public interests, infrastructure, financial, informational, and military assets are all potential targeting. Ambiguous rules of engagement.

5.2 Evolution of DoD Cyber Strategy:

In response to these new challenges, the DoD has gradually developed a strategy framework for understanding the nature of these threats, development appropriate policies for dealing with them,

[82] Chart by author, Glenn Voelz

Electronic copy available at: https://ssrn.com/abstract=2734336

and organizing the national security apparatus to support a range of possible responses. Much of the progress in this area has been reactive in nature, triggered by specific events serving to highlight the increasing complexity of the threat environment. Some of the more notable examples in recent years include:

- The 2007 attacks against the Estonian parliament, banks, ministries, newspapers, and media outlets, purportedly originating from Russia, that raised the question of whether NATO member countries would respond collectively to the DDoS attacks.

- A series of intrusions from 2007-2008 into defense contractor information systems, reportedly ex-filtrating several terabytes of data related to F-35 design information.

- A 2008 incident involving malicious computer code uploaded onto a Central Command classified network via flash drive placed by a foreign intelligence agency - a turning point in U.S. cyber-defense strategy and led, in part, the formation of U.S. Cyber Command.

- A 2015 North Korean attack on Sony Pictures, considered one of the most destructive cyber-attacks on a U.S. entity to date. This attack fueled an ongoing national discussion about the nature of the cyber threat and the need for improved cyber-security cooperation between government and the private sector.

These events, among others, have led to new policy initiatives and organizational changes within the DoD focused on cyber defense, network protection and DoD support to critical infrastructure security. More recently, this has included the explicit integration of offensive cyber capabilities into military doctrine and national security strategy. Several notable milestones in this evolution include:

- In 2006, the Joint Chiefs of Staff published the first National Military Strategy for Cyberspace Operations focused specifically on cyber security. The document characterized the cyberspace domain, identified threats and vulnerabilities, and proposed a strategic framework to assure U.S. military superiority in cyberspace.

- In 2007, the DoD launched the Defense Industrial Base (DIB) Cyber Security and Information Assurance program designed to increase the protection of sensitive information relating to defense technologies, weapons systems, policy and strategy development, and personnel.

- In 2009, Defense Secretary Gates ordered consolidation of the various DoD cyber task forces into a single four-star command, the U.S. Cyber Command, which began operations in May 2010 as part of the U.S. Strategic Command.

- In 2011, the DoD issued its first Strategy for Operating in Cyberspace. This strategy was significant as a policy document by outlining DoD's overall initiatives for cyber

Electronic copy available at: https://ssrn.com/abstract=2734336

space, and the recognition that DoD would treat cyberspace as a distinct operational domain (equivalent to air, land, maritime, and space) and organize, train, and equip forces so DoD could take full advantage of cyberspace's potential. However, this strategy document was vague on the use of offensive cyber capabilities and non-specific in the actors posing the greatest threats to U.S. interests.

- In 2015, the DoD issued an updated version of its Cyber Strategy, for the first time explicitly discussing the circumstances under which cyber-weapons could be used against an attacker. The document also explicitly named several countries presenting the greatest threat to U.S. interests in the cyber domain, including China, Russia, Iran and North Korea.

5.3 Overview of the 2015 DoD Cyber Strategy

The updated version of DoD's Cyber Strategy, released in 2015, outlined the evolving threats to U.S. interests, clarified the role of the DoD in countering these threats, and more clearly presented the range of possible policy responses to these threats. This has included an explicit statement describing a potential role for offensive cyber operations as part of a wider range of military response options. Several key points of the updated strategy document include:

- Highlighting that the nature of the threat and noting that "a disruptive, manipulative, or destructive cyber-attack could present a significant risk to U.S. economic and national security if lives are lost, property destroyed, policy objectives harmed, or economic interests affected."

- Clarifying bureaucratic roles and noting that the DoD, in concert with other agencies, is responsible for defending the U.S. homeland and U.S. interests from attack, including attacks that may occur in cyberspace.

- Presenting clear strategic goals focused on building capabilities for effective cyber-security and cyber operations to defend DoD networks, systems, and information; defend the nation against cyber-attacks of significant consequence; and support operational and contingency plans.

- Outlining five strategy goals for cyberspace missions, including:
  1. Build and maintain ready forces and capabilities to conduct cyberspace operations.
  2. Defend the DoD information network, secure DoD data, and mitigate risks to DoD missions.
  3. Be prepared to defend the U.S. homeland and U.S. vital interests from disruptive or destructive cyber-attacks of significant consequence.
  4. Build and maintain viable cyber options and plan to use those options to control conflict escalation and to shape the conflict environment at all stages.
  5. Build and maintain robust international alliances and partnerships to deter shared threats and increase international security and stability.

Electronic copy available at: https://ssrn.com/abstract=2734336

- Describing the structure of the "Cyber Mission Force" (CMF) within the DoD, comprised of nearly 6,200 military, civilian, and contractor support personnel from across the military departments and defense components.

- Acknowledging the challenge of deterrence in cyberspace, noting that due to the variety and number of state and non-state cyber actors in cyberspace and the relative availability of destructive cyber tools, an effective deterrence strategy requires a range of policies and capabilities to affect a state or non-state actors' behavior.

- Noting that attribution is a fundamental part of an effective cyber deterrence strategy as anonymity enables malicious cyber activity by state and non-state groups, thus requiring strong intelligence, forensics, and indications and warning capabilities to reduce anonymity in cyberspace and increase confidence in attribution.

- The strategy also clearly states that if directed, "DoD should be able to use cyber operations to disrupt an adversary's command and control networks, military-related critical infrastructure, and weapons capabilities."

While the 2011 defense cyber strategy was primarily defensive in focus, the updated 2015 version offers a more aggressive posture, noting that "during heightened tensions or outright hostilities, DoD must be able to provide the President with a wide range of options for managing conflict escalation. If directed, DoD should be able to use cyber operations to disrupt an adversary's command and control networks, military-related critical infrastructure, and weapons capabilities."[83] With regard to offensive cyber operations in the military context, recent legislation under Title 10 of the United States Code has supported this position and affirmed that "the Department of Defense has the capability, and upon direction by the President may conduct offensive operations in cyberspace to defend our Nation, Allies and interests, subject to the policy principles and legal regimes that the Department follows for kinetic capabilities, including the law of armed conflict and the War Powers Resolution."[84]

The updated strategy goes on to state that "there 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."[85] However, it still remains somewhat unclear how the U.S. might respond to cyber attacks from non-state actors against private corporations or individual U.S. citizens.

Publication of the 2015 document marks a significant evolution from previous DoD strategy.

[83] U.S. Department of Defense, *The Department of Defense*, 14.
[84] See Section 954, in the 2012 National Defense Authorization Act
[85] U.S. Department of Defense, *The Department of Defense.*

Electronic copy available at: https://ssrn.com/abstract=2734336

The most significant change is the explicit acknowledgement that offensive cyber operations have a clear role as part of U.S. military strategy. Furthermore, the language suggests that these capabilities could even be used in a preemptive manner or in a shaping role "during heightened tensions or outright hostilities." This broadened scope of utility suggests a potential role for cyber operations as part of a conventional military conflict, where capabilities could be directed against an adversary's command and control networks, military-related critical infrastructure, and weapons system. The document also provides greater detail on the bureaucratic structure of the government's evolving cyber force and how these entities work to protect military assets, economic interests, and critical infrastructure.

While the threats depicted in the strategy are significant, at least one knowledgeable analyst has suggested that the new strategy reflected a more sober estimate of the potential impact from such attacks, describing something less catastrophic than an imminent "cyber Pearl Harbor."[86] Despite greater clarity in the new strategy, some questions remain with regard to how this construct will be applied in specific scenarios, as well as thresholds for the use of offensive cyber weapons. For instance, how does the new strategy clarify the distinctions between various forms of cyber attack, such as between cyber-war, cyber-espionage, cyber-terrorism and cyber-crimes? Furthermore, how would the distinctions between these actions be relevant in determination of appropriate responses, either by conventional military instruments or by cyber weapons? Finally, under what scenarios could an adversary's cyber attack escalate into a conventional kinetic response? The answers to many of these questions are likely unknowable until confronted and clearly would vary depending upon specific circumstances, the impacts of the attacks, and the parties involved. For this reason, strategies are not expected to provide an exhaustive menu of response options for every conceivable scenario; however, they should generate planning scenarios and serve as a catalyst for developing a flexible range of policy options for decision-makers, including the capabilities and response tools necessary for dealing with an unpredictable set of contingencies. In this sense, the new strategy appears to offer forward movement in the policy debate on cyberwarfare based on serious consideration of how the U.S. might respond against a realistic range of threats.

[86] Herb Lin, "Two Observations About The New DOD Cyber Strategy," Lawfare Blog (blog), April 24 2015, www.lawfareblog.com/2015/04/two-observations-about-the-new-dod-cyber-strategy/.

Electronic copy available at: https://ssrn.com/abstract=2734336

References

Clapper, James R. 2015. Opening Statements to the Worldwide Threat Assessment Hearing. Senate Armed Services Committee, February 26. http://www.dni.gov/index.php/newsroom/testimonies/209-congressional-testimonies-2015/1175-dni-clapper-opening-statement-on-the-worldwide-threat-assessment-before-the-senate-armed-services-committee.

Lin, Herb. 2015. "Two Observations About The New DOD Cyber Strategy," *Lawfare Blog* (blog), April 24, 2015, www.lawfareblog.com/2015/04/two-observations-about-the-new-dod-cyber-strategy/.

Theohary, Catherine A. and John W. Rollins, *Cyberwarfare and Cyberterrorism: In Brief*. Washington DC: Congressional Research Service. http://fas.org/sgp/crs/natsec/R43955.pdf.

U.S. Department of Defense. 2015. *The Department of Defense Cyber Strategy*. Washington, D.C.: April. http://www.defense.gov/home/features/2015/0415_cyber-strategy/Final_2015_DoD_CYBER_STRATEGY_for_web.pdf.

Wood, Dakota L. and Heritage Foundation. 2015. *Index of U.S. Military Strength: Assessing America's Ability to Provide for the Common Defense*. Washington, DC: Heritage Foundation. Available at http://ims-2015.s3.amazonaws.com/2015_Index_of_US_Military_Strength_FINAL.pdf.

Electronic copy available at: https://ssrn.com/abstract=2734336

6. China's Perspective on Cyber Security[87]

Liu Yangyue

China has become an increasingly important player in global cyberspace. By the end of 2014, China's online population has risen to 649 million, accounting for 19% of Internet users worldwide as seen in Figure 1. Chinese corporations in the IT industry have been active in making transnational acquisitions, providing services and content overseas, and enhancing technological competitiveness. In the international politics of Internet governance, China's influence is also on the rise in recent years, as it seeks for greater participation and agenda-setting capabilities through multilateral institutions. So is its impact on security issues of cyber politics. Given that great power politics has largely defined and shaped the scope and meaning of security studies, it is necessary to examine China's perspective and stance on cyber security before conceptual and practical frameworks on this issue can be developed.[88] So far, China has not published or clarified its national strategy on cyber security. However, several aspects make its perspective unique and may facilitate a more comprehensive understanding of cyber security.

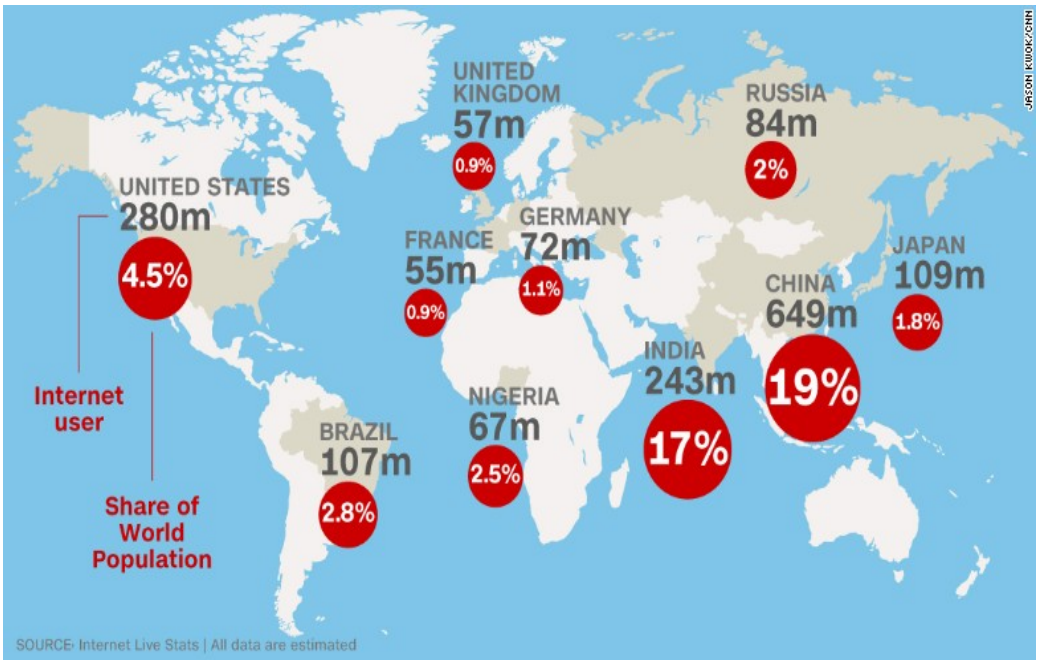


Figure 6.1
Global Internet usage
Source: Akamai (2014)

6.1 Internet Sovereignty

The first aspect concerns the notion of sovereignty. Unlike the Western mindset emphasizing the borderless nature of the Internet, what underlies the Chinese approach is the assumption that the

[87] Opinions and arguments expressed in this article are only personal, and do not represent any institution or government.
[88] Barry Buzan and Lene Hansen, *The Evolution of International Security Studies* (Cambridge, UK: Cambridge University Press, (2009), 50-53.

Electronic copy available at: https://ssrn.com/abstract=2734336

cyberspace is the natural extension, or a new dimension, of national sovereignty. In this sense nation-states should have unquestionable and paramount authority over the Internet system. In 2010, the Information Office of the State Council published a white paper on the *Internet in China*. Its content is to briefly outline China's stance on and understanding of Internet development and management. It contains a section called "Protecting Internet Security", in which it offers no clear definition of what Internet security is. However, it outlines three broad objectives of Internet security – respectively to "secure information flow", "combat computer crime" and "oppose all forms of computer hacking".[89]

These objectives make China's understanding of Internet security almost identical with other countries. But a notable difference lies in the emphasis on the Internet sovereignty. In the white paper, it proclaims "the Internet is an important infrastructure facility for the nation. Within Chinese territory the Internet is under the jurisdiction of Chinese sovereignty. The Internet sovereignty of China should be respected and protected". Meanwhile, "citizens of the People's Republic of China and foreign citizens, legal persons and other organizations within Chinese territory have the right and freedom to use the Internet; at the same time, they must obey the laws and regulations of China and conscientiously protect Internet security".[90]

By asserting sovereignty over cyberspace, China has re-framed the Western norm of a market-based, borderless Internet system to a reverse side that weighs national security over liberty and freedom. Moreover, the notion of Internet sovereignty would indicate a more centralized management system rather than distributed and decentralized governance. In fact, the design and structure of cyberspace do not necessarily favor a particular governance mode over others. As Rebecca MacKinnon has commented on Internet sovereignty, "it's a physical reality that web sites have to be hosted physically on computers that are located in some jurisdiction or another; they are operated by physical human beings who reside under a government jurisdiction and can thus be physically controlled when necessary; they are operated by businesses that have to be registered in one or more jurisdiction and their physical operations are subject to government regulation; and the Internet runs on networks that physically exist within or pass through nation-states".[91]

These connections between physical existence and virtual space mean that sovereignty can still be practiced, to some extent, in the cyber domain. A typical example refers to the way in which critical resources related to the operation of the Internet system are distributed and managed. On this score, the white paper outlines a hierarchical model of resource allocation by announcing, "the state telecommunications administration department is responsible for the administration of the Internet industry, including the administration of basic resources of the Internet such as domain names, IP addresses within China".[92] In China, the allocation and administration of domain names and IP addresses are controlled by the China Internet Network Information Center (CNNIC), which serves as a bureaucratic subordinate of the Ministry of Industry and Information Technology (MIIT). It should be noted that the global allocation of IP addresses is implemented in a geographic manner. It is divided into several Regional Internet Registries, with CNNIC being vertically affiliated to Asia-

[89] Information Office of the State Council of China. *The Internet in China*.. (2010): White paper available at http://news.xinhuanet.com/english2010/china/2010-06/08/c_13339232.htm.
[90] Ibid.
[91] Rebecca McKinnon, "China's Internet White Paper: networked authoritarianism in action," *RConversation* (blog), June 15, 2010, http://rconversation.blogs.com/rconversation/2010/06/chinas-internet-white-paper-networked-authoritarianism.html.
[92] Information Office, *The Internet in China*.

Electronic copy available at: https://ssrn.com/abstract=2734336

Pacific Network Information Center (APNIC) in Australia.

Ownership represents another mode of Internet sovereignty. In this regard, the Regulation on Telecommunications in China differentiates between two types of telecommunication services, basic telecom service (provision of public Internet infrastructure) and value-added service, and stipulates that companies in the basic telecom service should have at least 51% of their shares owned by the state. By putting service providers under national jurisdiction and control, this approach ensures that territoriality still matters when dealing with the virtual domain.

The notion of sovereignty has significant implications for the understanding of cyber security. It delineates a different boundary for where insecurity resides. It makes the distinction between globalized space and imagined national boundary. Sovereignty lies at the national side, which implicitly or explicitly portrays nation-states as the core referent object. Crucial factors that sustain the national image of cyber security point to the physical infrastructure of cyberspace which still operates within national borders, as well as the fundamental roles of territorial government that persist in the cyber domain.[93] On the other hand, cyber security also represents a novel global issue that occurs in a new arena of interactions.[94] Norms, practices, and institutions that manage security problems in the cyber domain have been fundamentally transformed due to the globalized feature of the cyber system.[95] The global governance of cyberspace may indicate the de facto elimination of cyber security boundary. This division, however, has also inhibited global efforts to establish a cohesive and coordinated framework that can better address cyber security problems. Recent development in global Internet governance regime, including events such as the WCIT in 2012 and NetMundial in 2014, has seen increasing disputes and disagreements about the future of Internet management.[96] How to bridge and conciliate these different visions would prove crucial in facilitating international cooperation on cyber security.

6.2 Information Security

Information security is another important element in China's perception of cyber security. Information security portrays information, per se, rather than its transmission as the major security concern. More specifically, it focuses primarily on the content and values embedded in the digital information.

The Administration of Internet Information and Service Procedures, promulgated in 2000, have broadly defined nine types of unlawful online content, including any content that opposes the fundamental principles of the Chinese Constitution, compromises state security, undermines national unity, and harms the dignity and interests of the state.[97] In an updated revision five year later, two additional materials are banned in cyberspace, namely any information that would incite illegal assemblies, marches and demonstrations, and that would represent the agendas of any illegal civil groups. In 2004, the China Internet Illegal Information Reporting Centre (CIIRC) was established to

[93] Daniel Drezner, "The Global Governance of the Internet: Bringing the State Back In," *Political Science Quarterly* 119, No. 3 (2004): 477-498; Jack L. Goldsmith and Tim Wu, *Who Controls the Internet?: Illusions of a Borderless World* (Oxford: Oxford University Press).
[94] Nazli Choucri, *Cyberpolitics in International Relations* (Cambridge, MA: The MIT Press, 2012).
[95] John Mathiason, *Internet Governance: The New Frontier of Global Institutions* (London: Routledge, 2008); Milton Mueller, *Networks and States: The Global Politics of Internet Governance* (Cambridge, MA: The MIT Press, 2010).
[96] Alexander Klimburg, "The Internet Yalta," *Center for a New American Security Commentary* (2013).
[97] Information Office, *The Internet in China*.

Electronic copy available at: https://ssrn.com/abstract=2734336

police the Internet space and identify any unlawful online materials.

To strengthen information security and enforce content regulation, China has built a multi-layered system. At the top level is a pervasive and effective filtering mechanism. Since 1998, the Ministry of Public Security has developed a powerful filtering and blocking system to monitor information flows between China and the outside world. This project, known as the Golden Shield, has become one of the most sophisticated and effective checkpoints in the information network. According to a report by the Open Net Initiative, although China is not the only country that deploys filtering techniques, "it is unique in the world for its system of Internet connections when triggered by a list of banned keywords".[98] This system is implemented at the backbone level, using a method named TCP resets. It can inspect the content of transmitted packets to uncover whether sensitive keywords are present and thus disrupt the connection. Using this filtering system, the government could contain undesired online discussion and communication, especially during politically sensitive periods or in times of emergency. This mechanism has also enabled the government to wipe out controversial news and anti-government speeches on the Internet ahead of important political events.

Below that level, responsibilities for regulating online information are delegated to content and service providers. For instance, major content providers are required to build internally a monitoring department. People in such department are in charge of examining and authorizing the information to be posted on their platform / website. Recent research by Gary King and his colleagues focus on the provider-level of information regulation.[99] It shows that the objective of regulation is mostly to reduce the likelihood of offline collective action mobilized through online platform. By contrast, criticism of the state or the Party has no evident effects on triggering regulatory measures. This finding indicates that the major concern of information security for China is to maintain social and political stability. On this score, political development in Egypt, Libya, Syria, Thailand and other countries may have served as a warning. Although information technologies may have empowered civil society vis-à-vis, the state, political order could be much more difficult to rebuild than collapse.

Teams of online commentators are also established by websites, media, government agencies as well as other state-sponsored institutions. Their duty is to guide and shape online opinion by countering rumors and developing positive arguments. The ultimate goal is to build a harmonious Internet space that supports rather than undermines existing socio-political structure. In late 2007, Cai Mingzhao, then-Vice Director of Information Office of State Council, emphasized that all forms of Chinese online media should "have a firm grasp of correct guidance, creating a favorable online opinion environment for the building of a harmonious society".[100] Down to the user-level, regulatory measures also include mechanisms such as real-name registration and filtering software.

The emphasis on information security makes China's perspective on cyber security different from that of the Western countries. While cyber security in the West is largely understood as concerning the rights of the individual, in the Chinese context it highlights collective, societal

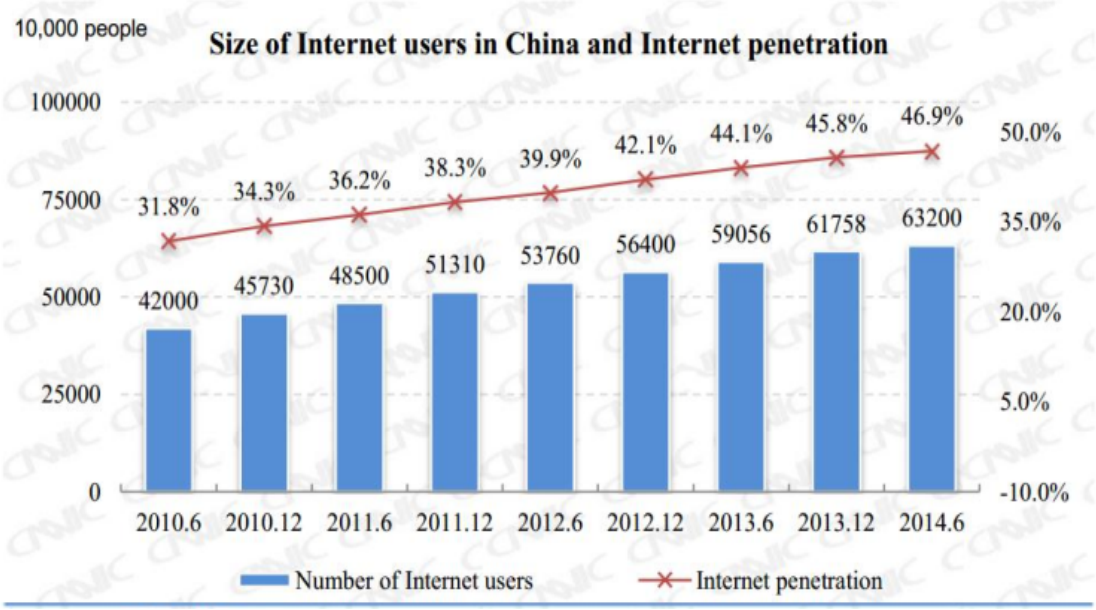
[98] "China's Green Dam: The Implications of Government Control Encroaching on the Home PC," Open Net Intitiative, accessed on…… https://opennet.net/chinas-green-dam-the-implications-government-control-encroaching-home-pc.
[99] Gary King, Jennifer Pan, and Margaret E. Roberts, "How Censorship in China Allows Government Criticism but Silences Collective Expression," *American Political Science Review* 107, no. 2 (2013): 1-18.
[100] David Bandurski, "State Council Vice-Minister reiterates control as top priority of Internet development in China," *China Media Project* (December 2007): http://cmp.hku.hk/2007/12/04/763/.

Electronic copy available at: https://ssrn.com/abstract=2734336

security, which places stability as a higher priority. Therefore, the 2010 white paper stresses "the free and safe flow of Internet information is integrated as a whole. On the premise of protecting the safe flow of Internet information, the free flow of Internet information may be realized".[101] This aspect of cyber security conception is not unique to China. Countries such as Russia also regard cyberspace as an integrated part of information space, where human cognitive processes interact with all kinds of information. In this sense, cyber security should not be separated from information security that deals with information systems as well as human minds.[102]

6.3 Development and Security

Last but not least, there is also a development aspect of cyber security. Over the past decade, the Internet in China has experienced high-speed growth (Figure-2). China now has the world's largest population – both online and offline. However, there is still a significant gap between China and more industrialized countries in terms of infrastructural development. Table 1 below exhibits several indicators related to Internet development among selected countries. It shows that China is still lagging behind in terms of secure servers, Internet hosts, and connection speed. For instance, China possesses only four secure Internet servers per million people, while that number is 1,306 for the United States, and 1,995 for South Korea. It is also noticeable that the use of pirated software prevails among Chinese Internet users (although not shown in the table). This has at least two implications for security: first is that the cyber environment in China is vulnerable. Akamai's quarterly reports of Internet attack traffic often identify China as one of the major attack sources (Table 1). But the nature of botnet suggests that the traced attack sources can also be (unwittingly) victims of intrusions and hijacks.



[101] Information Office, *The Internet in China*.
[102] Keir Giles and William Hagestad II, "Divided by a Common Language: Cyber Definitions in Chinese, Russian and English," in *5th International Conference on Cyber Conflict*, eds. K. Podins, J. Stinissen, and M. Maybaum (Tallinn: NATO CCD COE publications, 2013).

Electronic copy available at: https://ssrn.com/abstract=2734336

Source: CNNIC (2014)

Figure 6.2
China's Internet Growth

Table 1 Selected Indicators of Internet Development

	China	U.S.	Russia	Japan	S. Korea
Secure Internet servers (per 1m people)	4	1,306	51	737	1,995
Internet hosts (m.)	20.6	505	14.9	64.5	0.3
Average connection speed (Mbps) (2014Q4)	3.4	11.1	9	15.2	22.2
% of attack traffic (2014Q4)	41	13	3.2	0.8	2.8

Source: World Bank (2013); CIA World Factbook (2012); Akamai (2014)

Secondly, it creates a sense of technological dependency. For example, China has realized for a long time that in the areas of critical information technologies, such as CPU (central processing unit) and operating systems, it is highly dependent upon foreign companies. The risk of such dependency for national security has been recognized long ago. According to a survey conducted by a Chinese government agency, 97% of operating systems, 87% of servers, and a majority of industrial control systems currently used in China are overseas products. In a 2014 speech at the Leading Group for Informationization and Network Security, President Xi Jinping stresses that "cyber security is critical for national security and development … To build a cyber great power, China has to develop its own technologies".

In fact, China has made great efforts to promote security through indigenous innovations. One example is the WAPI standard. WAPI, short for WLAN Authentication and Privacy Infrastructure, is a Chinese-developed standard used for wireless networking system. It was allegedly designed to overcome the security deficiencies of the widely used Wi-Fi standard which was approved by the Institute of Electrical and Electronics Engineers (IEEE) in 1999. China initially announced in 2003 that all wireless devices sold in the Chinese market should support the WAPI standard. This move threatened the interests of the "Wi-Fi coalition" and provoked strong protest from the United States.[103] In 2004, the U.S. Secretary of Commerce Donald L. Evans, the Secretary of State Colin L. Powell, and the Trade Representative Robert B. Zoellick jointly sent a letter to their Chinese counterparts, complaining about the mandatory WAPI policy as a technological barrier to international trade.[104]

Under tremendous diplomatic pressures, China postponed the implementation of such a policy,

[103] Scott Kennedy, "The Political Economy of Standards Coalitions: Explaining China's Involvement in High-Tech Standards Wars", *Asia Policy* 2 (July 2006): 41-62.
[104] Sumner Lemon, "U.S. Government Voices Opposition to China's WLAN Standard", *IDG New Service* (March 2004): http://www.infoworld.com/t/networking/us-govt-voices-opposition-chinas-wlan-standard-740.

Electronic copy available at: https://ssrn.com/abstract=2734336

but later changed its tactic from internationalizing the WAPI standard to popularizing it first in the domestic market. Meanwhile China launched several prominent projects to make the WAPI a de facto mandated and industrialized standard, especially the extensive application of the WAPI in the 2008 Beijing Olympic Games and in the government procurement. This political effort paid off in 2009 when ten major countries, including the United States, and major industrial giants like Intel and Broadcom, had agreed to promote the WAPI as an international standard.[105] However, the Chinese government's effort to internationalize the WAPI standard suffered a temporary setback in mid-2011 when the United States rejected the visa of a Chinese expert who planned to raise the WAPI issue at the International Standard Organization's conference in San Diego.

The WAPI case is only one story of China's efforts to enhance indigenous innovations. Other achievements (as well as setbacks) have also occurred in the development of CPU, operating systems, technical standards, and high performance computers. The concern of technological independence has played an important role in China's policy of cyber security. Especially after the Snowden affair, Chinese government procurement has banned a number of overseas products, like the Windows 8 operating system, McAfee and other anti-virus software, CISCO's routers etc. And China is building an information technology review system to decide whether certain IT products are secure before they can be imported. All these developments are in the same line as China's pursuit of technological independence, which has been considered as a critical part of cyber security. In this sense, the recent U.S. embargo of processors widely used in the Chinese supercomputing industry may only validate and deepen China's concern about technological dependency.

6.4 Concluding Remarks

Although authoritative account in China has not provided a single, clarified (and publicly available) definition of cyber security, three aspects make its perspective distinctive. The elements of Internet sovereignty, information security and development are not separated from each other. Information security illustrates China's primary concern of Internet-related security problems, which prioritizes order and stability. Sovereignty represents an imagined domain, bounded by implicit and explicit nodes and scope, that falls under state jurisdiction and protection. Development, especially in terms of technological independence, is embedded in the conception of security and regarded as the most reliable and sustainable means to security.

Discussions above may have some interesting implications for the understanding of cyber security. While cyberspace is often perceived as a public domain where ownership and hierarchical authority do not apply, it is also an interactive system that has profound effects upon socio-political systems. Should inherent features of a socio-political system, such as culture, political order, and social stability, be part of the cyber security referent object? Should development and distribution be integrated into the conceptualization of cyber security? If so, what impacts would it bring to the current global regime of Internet governance? These questions are only a small fraction of puzzles emerging from the development of information technologies. It is of great necessity to enhance multilateral and multi-level dialogue and theory-building efforts to better understand the new issues in

[105] Iris Hong, "China's WAPi standard wins international support", *Telecomasia.net* (June 2009): http://www.telecomasia.net/content/chinas-wapi-standard-wins-international-support.

Electronic copy available at: https://ssrn.com/abstract=2734336

cyber politics.

As an added set of observations, the following is presented:

- Cyber Security and Global Governance
    - The white paper (2010) : “China maintains that all countries should, on the basis of **equality and mutual benefit**, actively conduct exchanges and cooperation in the Internet industry, jointly shoulder the responsibility of maintaining global Internet security… China holds that **the role of the UN** should be given full scope in international Internet administration… China maintains that all countries have equal rights in participating in the administration of the fundamental international resources of the Internet, and a **multilateral and transparent allocation system** should be established on the basis of the current management mode, so as to allocate those resources in a rational way and to promote the balanced development of the global Internet industry.”
- Cyber Security and Global Governance
    - China, Russia and other SCO members submitted the *International code of conduct for information security* in 2011 and 2015;
    - Code of Conduct: “Not to use information and communications technologies and information and communications networks to carry out activities which run counter to the task of maintaining international peace and security”; and not to “interfere in the internal affairs of other States or with the aim of undermining their political, economic and social stability”.
    - “All States must play the same role in, and carry equal responsibility for, international governance of the Internet, its security, continuity and stability of operation, and its development”.
- Cyber Security in Different Contexts
    - Cyber security for whom? Should culture, political order, social stability etc. be part of the cyber security referent object?
    - As the “freedom from fear” and “freedom from want” are intrinsically intertwined, the issue of development also plays a role in dealing with cyber security.
    - To what extent does power politics matter in global Internet governance?
- Sovereignty and Cyberspace
    - Krasner (1999) named four types of sovereignty: **domestic sovereignty** – actual control over a state; **interdependence sovereignty** – actual control of movement across state's borders; **international legal sovereignty** – formal recognition by other sovereign states; **Westphalian sovereignty** – lack of other authority over state than the domestic authority.
    - Is sovereignty feasible in cyberspace? Is cyberspace exerting a qualitative or quantitative impact on sovereignty

Electronic copy available at: https://ssrn.com/abstract=2734336

References

Bandurski, David. 2007. State Council Vice–Minister reiterates control as top priority of Internet development in China. *China Media Project*. (December): http://cmp.hku.hk/2007/12/04/763/.

Buzan, Barry and Lene Hansen. 2009. *The Evolution of International Security Studies*. Cambridge, UK: Cambridge University Press.

China Internet Network Information Center. 2000. *State Council Article 15, Administration of Internet Information and Service Procedures.* (September): http://www.cnnic.net.cn/html/Dir/2000/09/25/0652.htm.

China Internet Network Information Center. 2014. *Statistical Report on Internet Development in China*. http://www1.cnnic.cn/IDR/ReportDownloads/201411/P020141102574314897888.pdf.

Choucri, Nazli. 2012. *Cyberpolitics in International Relations*. Cambridge, MA: The MIT Press.

Drezner, Daniel. 2004. The Global Governance of the Internet: Bringing the State Back In. *Political Science Quarterly* 119 (3): 477-498.

Giles, Keir and William Hagestad II. 2013. Divided by a Common Language: Cyber Definitions in Chinese, Russian and English. In K. Podins, J. Stinissen, and M. Maybaum eds., 5th International Conference on Cyber Conflict, Tallinn: NATO CCD COE Publications. https://ccdcoe.org/cycon/2013/proceedings/d3r1s1_giles.pdf

Goldsmith, Jack L. and Tim Wu. 2006. *Who Controls the Internet?: Illusions of a Borderless World*. Oxford: Oxford University Press.

Hong, Iris. 2009. China's WAPI standard wins international support. Telecomasia.net (June): http://www.telecomasia.net/content/chinas-wapi-standard-wins-international-support.

Information Office of the State Council of China. 2010. *The Internet in China*. White paper available at: http://news.xinhuanet.com/english2010/china/2010-06/08/c_13339232.htm.

Kennedy, Scott. 2006. The Political Economy of Standards Coalitions: Explaining China's Involvement in High-Tech Standards Wars. *Asia Policy* 2 (July): 41-62.

King, Gary, Jennifer Pan, and Margaret Roberts. 2013. How Censorship in China Allows Government Criticism but Silences Collective Expression. *American Political Science Review*, 107 (May): 1-18.

Klimburg, Alexander. 2013. The Internet Yalta. *Center for a New American Security Commentary*. (February): http://www.cnas.org/sites/default/files/publications-pdf/CNAS_WCIT_commentary%20corrected%20%2803.27.13%29.pdf

Electronic copy available at: https://ssrn.com/abstract=2734336

Lemon, Sumner. 2004. U.S. Government Voices Opposition to China's WLAN Standard. *IDG News Service* (March): http://www.infoworld.com/t/networking/us-govt-voices-opposition-chinas-wlan-standard-740.

MacKinnon, Rebecca. 2010. China's Internet White Paper: networked authoritarianism in action. Web blog *RConversation*, June 15. http://rconversation.blogs.com/rconversation/2010/06/chinas-internet-white-paper-networked-authoritarianism.html.

Mathiason, John. 2008. *Internet Governance: The New Frontier of Global Institutions*. London: Routledge.

Mueller, Milton. 2010. *Networks and States: The Global Politics of Internet Governance*. Cambridge, MA: The MIT Press.

Open Net Initiative. "China's Green Dam: The Implications of Government Control Encroaching on the Home PC." Accessed on ……., https://opennet.net/chinas-green-dam-the-implications-government-control-encroaching-home-pc

Xinhuanet. 2014. Xi Jinping leads Internet security group. (February): http://news.xinhuanet.com/english/china/2014-02/27/c_133148273.htm.

Electronic copy available at: https://ssrn.com/abstract=2734336

7. Pursuing Deterrence Internationally in Cyberspace

Chrisma Jackson

Deterrence theory associated with warfare dates back centuries. In the Art of War, Sun Tzu said, "It is a doctrine of war not to assume the enemy will not come, but rather to rely on one's readiness to meet him; not to presume that he will not attack, but rather to make one's self invincible."[106] The concept of deterrence in the United States gained momentum and prominence during the Cold War. After the use of two nuclear weapons brought the end of World War II, the destruction and devastation demonstrated by these weapons brought deterrence theory into the forefront of U.S. DoD policy.

Deterrence theory is based on the idea of dissuading an adversary from taking action before a war has started. In 1959, Bernard Brodie stated, "A credible nuclear deterrent must always be ready, never used."[107] Later in 1966, Thomas Shelling highlighted deterrence as the "use of power to hurt is bargaining power is the foundation…and is most successful when it is held in reserve."[108] More recently, Graham Allison discussed the context of nuclear deterrence in the cold war: "…even during the most dangerous moments of the Cold War, a nation that attacked the United States with a nuclear armed ballistic missile would know that it had signed its own death certificate, since US retaliation would be immediate and overwhelming."[109] With deterrence theory a fundamental aspect of Cold War strategy, the "3 Cs" highlighted the theory's key characteristics:

- Clarity – bright lines and unacceptable consequences
- Capability – demonstrated capacity of technology able to demonstrate a response
- Credibility – an administration and government willing to respond when attacked[110]

In the decades following the cold war, the concept of deterrence extended as asymmetric attack/threat scenarios increased. A 2013 United Stated Space Command article described an extension of the use of Deterrence to Space. For these space-based applications, deterrence is defined as "the prevention of action by the existence of a credible threat of unacceptable counteraction and/or the belief that the cost of action outweighs the perceived benefits."[111] With this in mind, four safeguards were implemented to deter actions against U.S. space-based assets: 1) work international norms, 2) build coalitions to enhance security, 3) add resilience to architectures, and 4) prepare for an attack using defenses not necessarily in space.

This extension of deterrence theory into space leads us to comparisons with Cyber:

- Properties:
    1. Nuclear: Visible, visceral and overwhelming destruction.

[106] Tzu, Sun, 2009. *The Art of War*, Trans. Lionel Giles, file:///Users/User/Downloads/taowde.pdf.

[107] Bernard Brodie, *Strategy in the missile age* (Princeton, NJ: Princeton University Press, 1959).
[108] Thomas C. Schelling, *Arms and influence* (New Haven, CT: Yale University Press, 1966).
[109] Graham T. Allison, *Nuclear terrorism: the ultimate preventable catastrophe* (New York: Times Books/Henry Holt).
[110] Ibid; Graham T. Allison, personal interview,, Harvard Kennedy School, November, 2014.
[111] Karen Parrish, "Official describes Evolution of Space Deterrence," *American Forces Press Service* September 19 (2013): http://www.defense.gov/news/newsarticle.aspx?id=120818

Electronic copy available at: https://ssrn.com/abstract=2734336

2. Space: Non-visible attack interface, but destruction impacts military and civilians (particularly in the west).
3. Cyber: Non-visible attack interface with immediate impacts to civilians and military.

- Actions:
  1. Nuclear: Weapon ownership intended for the state with recent broad proliferation.
  2. Space: Investment initiated by nation states, but opening to civilian entrepreneurs.
  3. Cyber: (The Internet) Initiated as a government resource with growth and expansion dominated by academic and civilian entrepreneurs. In the last decade, international state controls vary greatly and will impact future technical direction.

Based on this brief comparison, the traditional notions of deterrence theory developed during the Cold War may not fully extend to other asymmetric threats (Space, Cyber), but that does not deny the successful historic use of deterrence the centuries before nuclear weapons and the notion of the use internationally with modern asymmetric threats.

7.1 Cyber Deterrence

With 90% of cyberspace networks and infrastructure owned and operated by private industry, deterrence in cyber is developing and evolving internationally.[112] In the U.S., the distributed nature of titles and authorities amongst government entities makes the defense and response to cyber attacks complex.

In 2013, the U.S. released Presidential Policy Directive/PPD-21 focused on Critical Infrastructure Security and Resilience which advances a national unity of effort to strengthen and maintain secure, functioning, and resilient critical infrastructure.[113] The nature of this document focused on a defensive cyber infrastructure for the United States inclusive of both civilian and military networks. Since the release of PPD-21, defensive cyber efforts have been implemented providing a foundation of protections for the U.S. networks (Figure 1).

[112] U.S. Department of Defense, "The Department of Defense Cyber Strategy," http://www.defense.gov/home/features/2015/0415_cyber-strategy/Final_2015_DoD_CYBER_STRATEGY_for_web.pdf (April 2015).
[113] U.S. Office of the President, "Presidential Policy Directive – Critical Infrastructure Security and Resilience," https://www.whitehouse.gov/the-press-office/2013/02/12/presidential-policy-directive-critical-infrastructure-security-and-resil (February 12, 2013).

Electronic copy available at: https://ssrn.com/abstract=2734336

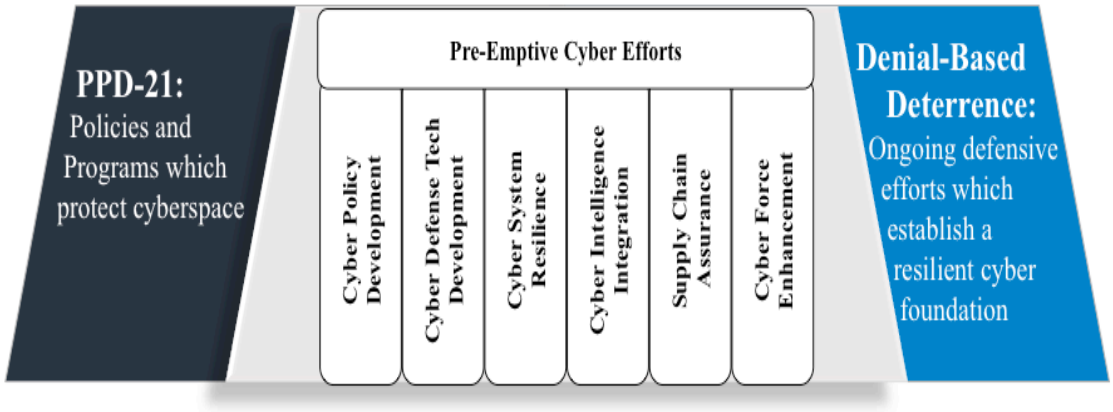


Figure 7.1
Defense/Denial Based Deterrence implemented via PPD-21.[114]

Recognizing that "making oneself invincible" in cyberspace is costly (and complete security cost prohibitive in the current model), the U.S. government is moving toward implementation of defenses via PPD-21 using cost/risk-based decision structure for cyber defenses that may be similar to that discussed by Wyss, et al.[115] In this structure, government decision-makers perform risk-based cost-benefit prioritization of security investments.

A coordinated risk-based, defensive structure thwarts some threats, but the porous nature of the internet and cost of cyber based defense drives a state away from utilizing a purely defensive deterrence structure and drives a state to consider a combined punishment-based/denial-based model (Figure 2). In a Punishment-based Deterrence scenario, the state responds with escalation following a cyber-based attack that is customized based on the attack. Response may include, but is not limited to, criminal action (naming and shaming, fines, incarceration), diplomatic action (demarche), economic sanctions (banking restrictions, trade bans), offensive cyber response (DDOS), coordinated ally response, and kinetic response.

In this model, a cyberattack may see immediate and overwhelming force in retaliation to the attack.

[114] Heather Blackwell, Chrisma Jackson, and Jennifer McCann, An Analytic Framework for United States Cyber Deterrence," Research Project Presentation on April 28, 2015. Harvard Kennedy School Research Paper for National Security Fellows.
[115] Gregory D. Wyss, John P. Hinton, Katherine Dunphy-Guzman, John Clem, John Darby, Consuelo Silva, and Kim Mitchiner, "Risk-Based Cost-Benefit Analysis for Security Assessment Problems," *Security Technology (ICSST)*, 2001 IEEE International Carnahan Conference on Security Technology, San Jose, CA, Oct 5-8, 2010, 286-295.

Electronic copy available at: https://ssrn.com/abstract=2734336

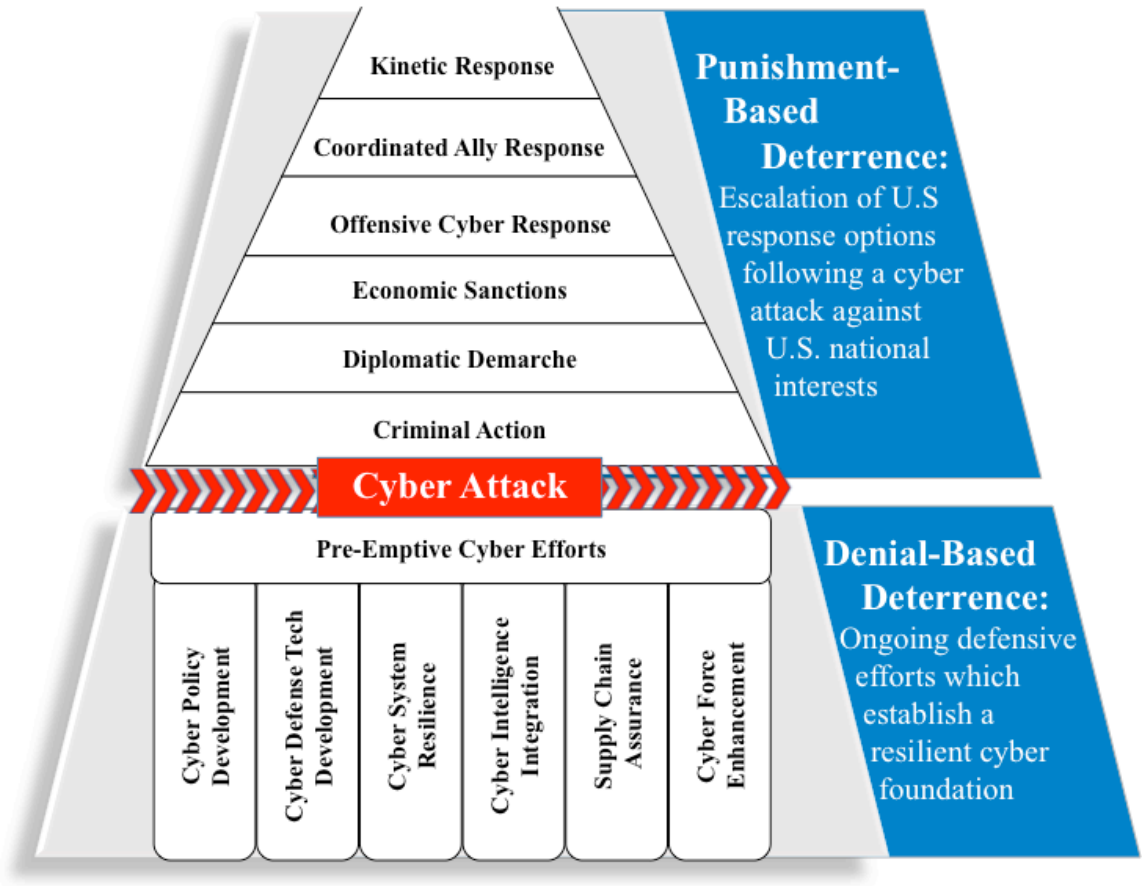


Figure 7.2
Combined Punishment/Denial Framework for Cyber Deterrence

7.2 International Demonstrations of Force or Deterrence: International Examples

The notion of the extension of deterrence to cyber has been discussed academically, but discussions at the state level have been limited. Based on recent attacks/ responses as well as media reports, U.S., Russia and China appear to be building their attack/response profiles.

In the U.S., several recent incidents and reports confirm responses and demonstrations of force may be highlighted. In 2012, the U.S. Marines confirmed the use of cyberattacks in Afghanistan including use of tools to "get inside his (enemy) nets, infect his command-and-control, and in fact defend myself against his almost constant incursions to get inside my wire, to affect my operations."[116] Late in 2014, international headlines were filled with the news related to the North Korean attacks on Sony Pictures Entertainment. In response for those attacks, the U.S reportedly is leading a criminal investigation, diplomatic demarche, diplomatic sanctions, offensive cyber attacks, and international coordination (with China).[117] In the spring of 2015, President Obama and Prime

[116] Raphael Satter, "U.S. General: We hacked the enemy in Afghanistan," *Associated Press* August 24, 2012 on USA Today, http://usatoday30.usatoday.com/news/military/story/2012-08-24/afghan-cyberattack/57295168/1.
[117] David Robb, "Sony Hack: A Timeline," *Deadline.com*, http://deadline.com/2014/12/sony-hack-timeline-any-pascal-the-interview-north-korea-1201325501/(accessed December 19, 2014); Jim Acosta and kevin Liptak, "U.S. Slaps New Sanctions on North Korea after Sony Hack," *CNN.com*, http://www.cnn.com/2015/01/02/politics/new-sanctions-for-north-korea-after-sony-hack/index.html(accessed March 7,

Electronic copy available at: https://ssrn.com/abstract=2734336

Minister Cameron announced a cooperative cyber alliance and "joint war games" with the U.K.[118]

Coordinated cyberattacks on Estonia, originating from Russia, in 2007 disrupted the communications and operations of the banks, parliament, ministries, newspapers, and TV in the state.[119] These attacks were a clear demonstration of offensive capability and force. Following these attacks in 2013, Russia announced the creation of a Cyber Army including the establishment of a Cyber Defence Centre citing a "need to gather intelligence as with traditional espionage; the ability to disrupt communications to hamper conventional forces, and also the ability to deliver cyber-assaults on critical infrastructure – including the banking sector…".[120]

China has had an active government cyber program restricting internal access to parts of the larger internet, nicknamed the "Great Firewall of China," for years, but most recent reports in a March 2015 PLA publication openly discuss specialized units devoted to wage war on computer networks. The units include:

- Specialized military forces - fighting offensively and defensively on networks.
- Experts from civil society organizations - Ministry of State Security (equivalent to China's CIA), and the Ministry of Public Security (equivalent to the FBI) – who are authorized to conduct military leadership network operations.
- External entities - non-government entities (state-sponsored hackers) mobilized for network warfare operations.[121]

Following the March publication, the new DDoS tool, nicknamed "The Great Cannon", was hijacking traffic to (and presumably from) individually IP addresses whereas restricting users from accessing those addresses on the net. "Where the Great Firewall was a tool for largely passive censorship – preventing access to material and providing the Chinese state with the ability to spy on its residents – the Great Cannon provides the ability to effectively rewrite the internet on the fly."[122]

As we look across the world, the build-up and leveraging of cyber as a platform is being leveraged internationally amongst the major powers: U.S. Russia, and China. Acts demonstrating the three "Cs": demonstrations of technology/joint war games (Capability), defining clear lines of attack (Clarity), and the willingness of governments to respond via use of force (Credibility) draw new meaning and extension to the use of deterrence theory.

2015); Mike Chinoy, "A Cyber Conflict with North Korea is 'Dangerous Uncharted Territory'," *CNN.com,* http://www.cnn.com/2014/12/23/world/asia/north-korea-cyber-conflict-chinoy-qa/index.html (accessed March 7, 2015); Nicole Perlroth and David E. Sanger, "North Koreas Loses its Link to the Internet," *The New York Times* December 22, 2014, http://www.nytimes.com/2014/12/23/world/asia/attack-is-suspected-as-north-korean-internet-collapses.html.

[118] U.S. Office of the President, "FACT SHEET: U.S.-United Kingdom Cybersecurity Cooperation," *Office of the Press Secretary* January 16, 2015, https://www.whitehouse.gov/the-press-office/2015/01/16/fact-sheet-us-united-kingdom-cybersecurity-cooperation.

[119] Charles Clover, "Kremlin-backed group behind Estonia cyber blitz," *Financial Times* March 11, 2009, http://www.ft.com/cms/s/0/57536d5a-0ddc-11de-8ea3-0000779fd2ac.html.

[120] Eugene Gerden, "$500 million for new Russian cyber army," *SC Magazine* November 6, 2014, http://www.scmagazineuk.com/500-million-for-new-russian-cyber-army/article/381720/.

[121] Mohit Kumar, "China finally admits it has Army of Hackers," *The Hacker News* March 19, 2015, http://thehackernews.com/2015/03/china-cyber-army.html.

[122] Alex Hern, ""Great Cannon of China" turns internet users in to weapon of cyberwar," *The Guardian* April 13, 2015, http://www.theguardian.com/technology/2015/apr/13/great-cannon-china-internet-users-weapon-cyberwar.

Electronic copy available at: https://ssrn.com/abstract=2734336

References

Acosta, Jim and Kevin Liptak. 2015. U.S. Slaps New Sanctions on North Korea after Sony Hack. *CNN.com*. Accessed March 7, 2015, http://www.cnn.com/2015/01/02/politics/new-sanctions-for-north-korea-after-sony-hack/index.html.

Allison, Graham T. 2004. *Nuclear terrorism: the ultimate preventable catastrophe*. New York: Times Books/Henry Holt.

Allison, Graham. 2014. Interview with Heather Blackwell, Chrisma Jackson, and Jennifer McCann Personal interview. Harvard Kennedy School, Cambridge, MA, November 4.

Blackwell, Heather, Chrisma Jackson, and Jennifer McCann. 2015. An Analytic Framework for United States Cyber Deterrence. Research Project Presentation on April 28. Harvard Kennedy School Research Paper for National Security Fellows.

Brodie, Bernard. 1959. *Strategy in the missile age*. Princeton, N.J.: Princeton University Press.

Chinoy, Mike. 2015. A Cyber Conflict with North Korea Is 'Dangerous Uncharted Territory'. *CNN.com*. Accessed March 7, 2015. http://www.cnn.com/2014/12/23/world/asia/north-korea-cyber-conflict-chinoy-qa/index.html.

Charles Clover, "Kremlin-backed group behind Estonia cyber blitz," *Financial Times* March 11, 2009, http://www.ft.com/cms/s/0/57536d5a-0ddc-11de-8ea3-0000779fd2ac.html.

Gerden, Eugene. 2014. $500 million for new Russian cyber army. *SC Magazine* November 6. http://www.scmagazineuk.com/500-million-for-new-russian-cyber-army/article/381720/.

Hern, Alex. 2015. "Great Cannon of China" turns internet users in to weapon of cyberwar. *The Guardian* April 13. http://www.theguardian.com/technology/2015/apr/13/great-cannon-china-internet-users-weapon-cyberwar.

Kumar, Mohit. 2015. China finally admits it has Army of Hackers. *The Hacker News* March 19. http://thehackernews.com/2015/03/china-cyber-army.html.

Parrish, Karen. 2013. Official describes Evolution of Space Deterrence. *American Forces Press Service*. U.S. Department of Defense. http://www.defense.gov/news/newsarticle.aspx?id=120818.

Perlroth, Nicole and David E. Sanger. 2014. North Korea Loses Its Link to the Internet. *The New York Times*. December 22. http://www.nytimes.com/2014/12/23/world/asia/attack-is-suspected-as-north-korean-internet-collapses.html.

Electronic copy available at: https://ssrn.com/abstract=2734336

Robb, David. 2014. Sony Hack: A Timeline. *Deadline.com*. Accessed December 19, 2014, http://deadline.com/2014/12/sony-hack-timeline-any-pascal-the-interview-north-korea-1201325501/.

Satter, Raphael. 2012. U.S. general: We hacked the enemy in Afghanistan. *Associated Press*. USA Today. http://usatoday30.usatoday.com/news/military/story/2012-08-24/afghan-cyberattack/57295168/1.

Schelling, Thomas C. 1966. *Arms and influence*. New Haven: Yale University Press.
Tzu, Sun, *The Art of War*, Trans. Lionel Giles, 2009, file:///Users/User/Downloads/taowde.pdf.

U.S. Department of Defense. 2015. The Department of Defense Cyber Strategy. Department of Defense: April. http://www.defense.gov/home/features/2015/0415_cyber-strategy/Final_2015_DoD_CYBER_STRATEGY_for_web.pdf.

U.S. Office of the President. 2013. Presidential Policy Directive -- Critical Infrastructure Security and Resilience. February, 12. https://www.whitehouse.gov/the-press-office/2013/02/12/presidential-policy-directive-critical-infrastructure-security-and-resil.

U.S. Office of the President. 2015. FACT SHEET: U.S.-United Kingdom Cybersecurity Cooperation. *Office of the Press Secretary*, January 16. https://www.whitehouse.gov/the-press-office/2015/01/16/fact-sheet-us-united-kingdom-cybersecurity-cooperation.

Wyss, Gregory D., John P. Hinton, Katherine Dunphy-Guzman, John Clem, John Darby, Consuelo Silva, and Kim Mitchiner. 2011. Risk-Based Cost-Benefit Analysis for Security Assessment Problems. Security Technology (ICSST), 2001 IEEE International Carnahan Conference on Security Technology, San Jose, CA, Oct 5-8, 2010, 286-295.

Electronic copy available at: https://ssrn.com/abstract=2734336

8. Is Deterrence Possible in Cyber Warfare?

Brooke Gier

While it may not seem like it at face value, nuclear warfare and cyber warfare have a lot in common. Both exist in domains characterized by the security dilemma, offense-defense balance, and the urge for preemptive strikes. Both are unconventional and have the capability to cause enormous damage to a state. Deterrence – the aim to prevent an adversary from attacking with the threat of retaliation - was utilized as a strategic policy answer to the nuclear tension between the Soviet Union and the United States during the Cold War. Similarly, deterrence seems like a viable option to prevent cyber attacks currently.

There are several problems with the use of deterrence, however. First, deterrence requires communication in order to work – the threat has to be communicated to the adversary, otherwise he will not know it even exists – and this communication seems to be unavailable during cyber conflict. Second, unlike nuclear warfare, cyber conflict has a range of severity – it can be harmless, or it can be catastrophic. Thus, states lose credibility - another needed component of deterrence – to punish an aggressor when the aggressor has committed a "harmless" act because it is unreasonable to do so. Third, terrorist groups and individuals have the capacity to conduct cyber warfare, unlike nuclear warfare. Thus, a rational actor – another need for deterrence – is removed. Despite these difficulties, state leaders do need to formulate an international agreement to address the cyber realm, so that in the case a cyber attack does occur, there is a plan to address it.

8.1 Cyber Definitions

There are numerous definitions floating around for cyberspace, cyber security, and cyber warfare. This paper identifies cyberspace to include both the physical and syntactic layer, as well as distinguishes cyber warfare from cyber conflict or incident. Cyber conflict is "the use of computational technologies in cyberspace for malevolent and destructive purposes in order to impact, change, or modify diplomatic and military interactions between entities short of war and away from the battlefield."[123] Cyber warfare falls under cyber conflict, but involves attacks that are generally much more severe, malicious, and originate from a state or organization (such as a terrorist organization) against another state or organization.

8.2 The Structure of International Relations

To continue with this paper, it is important to lay down fundamental concepts of the political and cyber realm. According to traditional realist theory,[124] three fundamental aspects characterize the international system: anarchy, self-help, and sovereignty. There is no official hierarchy or governing structure over states, and each state must work for its own survival. States are sovereign over their own land, people, and resources, and externally are considered "equals" when it comes to international law.[125] States devise grand strategies- a state's theory about how it can best devote its

[123] Brandon Valeriano and Ryan C Maness, "The Dynamics of Cyber Conflict Between Rival Antagonists, 2001-2011," *Journal of Peace Research* 51(2014): 348.
[124] Realist theory is focused on because of its significance in nuclear deterrence strategy and theory.
[125] Kenneth Waltz, *Theory of International Politics* (Reading, MA: Addison-Wesley Pub., 1979), 102-116.

Electronic copy available at: https://ssrn.com/abstract=2734336

resources to achieving its objectives– and incorporate military doctrine – a subcomponent of grand strategy that deals explicitly with military means - to ensure the security of the state.[126]

According to Barry Posen, states can adopt three different types of military doctrine.[127] An offensive doctrine aims to disarm or destroy the enemy, while a defensive doctrine aims to deny the enemy from achieving the objective he seeks. A deterrent doctrine aims to punish an aggressor - to raise his costs without reference to reducing one's own. This leaves a state vulnerable to enemy attack because it normally lacks defensive capability.[128] Normally states adopt some kind of mixture of these doctrines.

According to traditional realist theory, security dilemmas are an inherent part of the international system. By increasing one's own security, one decreases the security of others. This leads states to respond with similar measures, which leads to arms races and potential military conflicts. The offense-defense balance further affects security dilemmas. If offense has the advantage, a security dilemma is more likely to ensue more quickly and dangerously.[129] Weapon technology adopted matters. For example, building a moat and barbed wire is not going to make a neighbor state as nervous as mobilizing troops and creating weapons that can be used both defensively and offensively. When offense has the advantage, this normally leads to preemptive strikes because speed is of the essence.[130]

8.3 Nuclear Strategy: Deterrence

After the advent of the nuclear bomb and the beginning of the Cold War, deterrence became the cornerstone of U.S. strategic and military doctrine to prevent preemptive strikes. Deterrence requires capability, credibility, and communication. A state must have the ability to punish an aggressor, the credibility to actually follow through with the threat, and communicate this to its adversary.[131] The infamous Mutually Assured Destruction policy adopted in the 1960s was the fruit of the security dilemma and nuclear deterrence. It assumed that each belligerent had enough nuclear capability to destroy the other side, and the other side could also destroy its enemy if attacked.[132] It, thus, had several requirements in order to be effective: a second strike capability and a rational enemy. If states did not have a second strike capability, then they would be motivated to preemptively strike their enemy in a "use it or lose it" situation. The other side also had to be rational – in other words, he had to also desire to avoid nuclear warfare.

Nuclear strategy and deterrence have potential applications to cybersecurity. Military planners like to compare cyber weapons to nuclear weapons because each can cause massive, strategic-level damage and both require presidential authority to use.[133] Cyber warfare, like nuclear warfare, has the possibility to be avoided through deterrence. It has been widely noted that offense has the advantage

[126] Barry Posen, *The Sources of Military Doctrine: France, Britain, and Germany between the World Wars* (Ithaca, NY: Cornell University Press, 1984), 24.
[127] Ibid.
[128] Ibid.
[129] Charles L. Glaser and Chaim Kaufman, "What Is the Offense-Defense Balance and Can We Measure It?" *International Security* 22 (1998): 44-82.
[130] Ibid.
[131] Patrick M. Morgan, "Applicability of Traditional Deterrence Concepts and Theory to the Cyber Realm" in *Proceedings of a Workshop on Deterring CyberAttacks: Informing Strategies and Developing Options for U.S. Policy*, 55-77, Washington, DC: National Academies Press.
[132] Ibid.
[133] Shane Harris, *@ War: The Rise of the Military-Internet Complex* (New York: Houghton Mifflin Harcourt Publishing, 2014), 48-50.

Electronic copy available at: https://ssrn.com/abstract=2734336

when it comes to cyber warfare; it is easier to attack than defend against cyber attacks.[134] An attack need only succeed once, whilst defense must succeed every time. Additionally, there are numerous malware and potential cyber attacks being created on a daily basis - defense has the hard job of keeping up with these developments.[135] Therefore, theoretically preemptive strikes will be more likely, especially as cyber warfare becomes more integrated into military doctrine in the future.

8.4 The Schriever Wargame Implications for Deterrence

In fact, this has proven the case when the annual Schriever Wargame played out a cyber war scenario. Each year, a game is held premising a strategy issue currently vexing U.S. forces, with participants from more than thirty U.S government agencies including the Intelligence Community, Defense, as well as private sector actors like executives from technology companies.[136] In 2010, the game was premised on cyber warfare – an adversary in the Pacific region launched a crippling cyber attack against a U.S. ally, the ally invoked its mutual defense agreement, and the United States had to respond. Yet, before the United States could make its first move, the adversary struck preemptively to block the US forces' access to the computer networks they needed to communicate and send orders.[137]

Conventional blockades allow belligerents the ability to communicate to each other by flashing lights or hailing to each other over radio frequency – that can give warnings and signal assertive actions, but fall short of actual fire and lethal action. In the game, however, the participants did not know how to communicate – they only knew how to attempt to destroy the adversary's network.[138] Deterrence failed – assuming deterrence had even existed in the first place (it was not clear that the other side even believed in it.) The adversary's next step was to push U.S. satellites out of orbit.[139] The participants playing the U.S. side became confused and disorganized – not sure what to do short of launching a full-scale war. They realized that there were no cyber war agreements with foreign allies, and thus no "road map" for an international response.[140] Ultimately, the mock game persuaded U.S. civilian and military officials to reassess how they looked at cyber warfare and their readiness for it.

Harris argues that there is a clear set of steps that belligerents can take to avoid a nuclear war.[141] Throughout the Cold War, U.S. and Soviet officials created and demonstrated new types of missiles, as well as discussed nuclear weapons in speeches and public statements.[142] These steps did not exist or emerge during the war simulation game – there was no communication whatsoever. That is not to say these steps are not possible in the realistic future, but since integrating the cyber realm into military doctrine and grand strategy are still in its beginning stages, they have not been created yet. Either way, the necessary component of communication for cyber deterrence is lacking.

8.5 Analysis of Actual Cyber Conflict and Implications for Deterrence

Interestingly, however, the Schriever Wargame seems to have represented an anomaly from

[134] Nazli Choucri quotes James R. Gosler in *Cyberpolitics in International Relations* (Cambridge, MA: The MIT Press, 2012), 149.
[135] Ibid., 144.
[136] Harris, *@ War,* 49-50.
[137] Ibid., 50.
[138] Ibid.
[139] Ibid., 49.
[140] Ibid.
[141] Ibid., 49-50.
[142] Ibid.

Electronic copy available at: https://ssrn.com/abstract=2734336

current cyber international relations. Brandon Valeriano and Ryan C. Maness conducted a research study looking at how serious the cyber threat currently is between state rivals, and found very different results than the scenario presented to the participants at the Schriever Wargame. They developed a scale to assess cyber incident damages on a scale from one to five. One was a nuisance and harmless (like defacing websites) while five was "escalated dramatic effect on a country."[143] First, they found that very few states actually fight cyber battles. They expected to find one incident/dispute per year for each rivalry dyad and actually found less than that.[144] Second, there were few and far in between instances of relative severity, and none of them were so severe as to provoke military action. The highest severity was a three, and this only occurred in 13% of cases. The average severity was a 1.62.[145] The occurrence of a cyber incident was not only rare – it was unlikely to be severe at all.

Finally, they found that China was the main instigator behind many of the attacks. They noted that cyber conflicts tended to remain regional, but the most active cyber relationship was one with global implications: the outlier of the United States and China. China had initiated a cyber conflict 20 times with the United States within the eleven-year period, while the United States only initiated two. China's motivation appears to be stealing sensitive or secret information.[146] These numbers show a couple things. First, the United States' well-known cyber offense capabilities failed to deter China from cyber initiations and second, the United States has shown great restraint in deciding not to retaliate against China.

Valeriano and Maness's study shows fundamental differences between nuclear deterrence and cyber deterrence. Their inherent nature sets them apart. There is no range of severity for a nuclear attack – all nuclear attacks start on the catastrophic and disastrous level and continue to get worse from there. There is, however, a range of severity for cyber incidents. States can carry out smaller attacks that are nuisances and relatively harmless, rather than actual threats to national security.[147] This has several implications. As Harris points out, cyber conflicts lack the necessary communication component of deterrence - the "dance steps" policymakers can take to send signals. Yet even more importantly, they also seem to lack the necessary credibility requirement for deterrence.

Cyber conflicts, unlike nuclear conflicts, *can* be small and harmless and this means that one of the crucial elements of deterrence is undermined: credibility. Namely, the United States is not going to provoke a tantamount and horrendous war because China hacked into the State Department and looked at some secret files.[148] China *knows* this – and thus, the U.S. loses its credibility to threaten a disastrous punishment. Deterrence will fail until a certain point – the point at which the cyber incident becomes serious enough to call for a substantial national and possibly military response to the incident. So what does this mean for U.S. policymakers? While it is important to have an operational plan ready in case a country were to spontaneously launch a devastating cyber attack on the United States, it seems more worthwhile to invest resources into handling more realistic cyber conflicts – on a range of severity levels.

[143] Valeriano and Maness, "The Dynamics of Cyber Conflict," 353.
[144] Ibid., 355.
[145] Ibid.
[146] Ibid., 356.
[147] Valeriano and Maness, "The Dynamics of Cyber," 350-357.
[148] Ibid., 356-357.

Electronic copy available at: https://ssrn.com/abstract=2734336

8.6 The Trouble of Non-State Actors

Additionally, some scholars worry that terrorist groups can gain control over nuclear weapons (whether that is likely or not remains debatable);[149] however, the same can surely be said for terrorist groups and cyber warfare. Unlike nuclear weapons, cyber warfare is easily accessible to individuals and organizations.[150] The extent of the amount of damage they can cause remains unknown, yet given the constant development of cyber offensive capabilities, their ability to cause severe damage in the future is probable.

Many have already learned how to use the cyber arena to their advantage.[151] Cyber warfare in the hands of terrorist groups removes one of the main components for a deterrent policy like MAD to work – a rational actor. As U.S. policymakers move forward, this is one more important element to keep in mind.

8.7 The Importance of International Regulation

Ultimately, just because cyber incidents are not currently severe and commonplace does not prevent that from happening in the future. The Schriever Wargame showed it is imperative that major powers come together and decide an international agreement on cyber warfare for several reasons. Firstly, to ideally prevent preemptive strikes from being taken in the first place and secondly, so there are international responses in place to address such attacks in case they should ever occur. Richard Price argues that unconventional weapons are not inherently unconventional – social norms deem them so, established by state leaders.[152] They have an institutionalized stigma, and there are laws that forbade their use and policies set up to address if they are used.

Cyber weapons are arguably unconventional – they add an entire new dimension to warfare and have the ability to negatively impact entire populations at one time. Therefore, an international agreement is imperative for cyber weapons, especially as their capabilities and technologies develop. Key rival leaders need to meet and assess the different threats cyber warfare currently has upon their respective nations, and collectively decide what they believe is allowable and what they believe is not. Deterrence may not work for the low-level cases of cyber incidents, but it can surely work for the severe and devastating attacks. This needs to be established before they can be allowed to happen, and set off a chain reaction of devastating attacks. While this may not directly address the potential of terrorist groups and individuals, it is an important start that can help states respond to such a threat, should it ever occur.

[149] Scott Sagan is the most notable.
[150] Nazli Choucri and David D. Clark, "Integrating Cyberspace and International Relations: The Co-Evolution Dilemma," *Version 8-25 for internal ECIR review* (August 2011), 1-4.
[151] Choucri, *Cyberpolitics,* 152.
[152] Richard Price, *The Chemical Weapons Taboo*, (Ithaca, NY: Cornell University Press), 70-100.

Electronic copy available at: https://ssrn.com/abstract=2734336

References

Choucri, Nazli. 2012. *Cyberpolitics in International Relations.* Cambridge, MA: The MIT Press.

Choucri, Nazli and David D. Clark. 2011. Integrating Cyberspace and International Relations: The Co-Evolution Dilemma. *Version 8-25 for internal ECIR review* (August 2011), 1-4.

Glaser, Charles L. and Chaim Kaufman. 1998. What Is the Offense-Defense Balance and How Can We Measure It? *International Security* 22 (Spring): 44-82.

Harris, Shane. 2014. *@ War: The Rise of the Military-Internet Complex.* New York: Houghton Mifflin Harcourt Publishing.

Morgan, Patrick M. 2010. Applicability of Traditional Deterrence Concepts and Theory to the Cyber Realm. In *Proceedings of a Workshop on Deterring CyberAttacks: Informing Strategies and Developing Options for U.S. Policy*, 55-77, Washington, DC: National Academies Press.

Posen, Barry. 1984. *The Sources of Military Doctrine: France, Britain, and Germany between the World Wars*. Ithaca, NY: Cornell University Press.

Price, Richard M. 1997. *The Chemical Weapons Taboo*. Ithaca, NY: Cornell University Press.
Valeriano, Brandon and Ryan C Maness. 2014. "The Dynamics of Cyber Conflict Between Rival Antagonists, 2001-2011," *Journal of Peace Research* 51 (May): 347 – 360.

Waltz, Kenneth N. 1979. *Theory of international politics*. Reading, MA: Addison-Wesley Pub. Co.

Electronic copy available at: https://ssrn.com/abstract=2734336

9. A Theoretical Framework for Analyzing Interactions between Contemporary Transnational Activism and Digital Communication

Vivian Peron

The aim of this text is to contribute to cyber security studies workshop from a social perspective through consideration of the role of political groups or social movements and their potential impacts on international relations. Specifically, this study shows the cyberspace effects on transnational activism's dynamics considering digital communication's uses by activists.

Activism is a role assumed by individuals or collective actors either to resist what they consider to be a political wrong or to act to bring about political change through either contained or transgressive tactics. It is a process defined by a political cause which may originate online or not. An activist therefore may be a member of a social movement, popular struggle, trade union, collective, network, NGO, or civic or religious organization, a scholar or student, or an individual unaffiliated with any group. Transnational activism is the term used to indicate coordinated international campaigns on the part of networks of activists against international actors, other states, or international institutions.[153]

Even though there is a traditional set of studies in Social Sciences related to transnational activism, this conceptualization has been expanded and reinforced by inserting new elements and actors in these communicative processes through the social use of new technologies such as the Internet. Some events in the first decades of the 21st century are emblematic of this change, such as the Arab Spring, Al Qaeda, and WikiLeaks. These phenomena are different examples of transnational activism's dynamics and illustrate how their actions impact and may redefine security and stability in international relations. For this reason, this study focuses on the role of digital communication in the dynamics of contemporary transnational activism.

This study is divided into three parts. Firstly, this study defines cyberspace and digital communication through a social perspective. From this conceptual background, it is possible to explain the main cyberspace effects on social practices. Secondly, the study organizes the activism's dynamics into six stages: Arrangement of the cause, individual engagement, action planning, execution of actions, visibility production and reaction or counter-attacks. Thirdly, the preliminary analysis shows cyber effects on transnational activism's dynamic using illustrations from three different cases: the Arab Spring, Al Qaeda, and WikiLeaks.

[153] Margaret E. Keck and Kathryn Sikkink, *Activists beyond Borders: Advocacy Networks in International Politics* (Ithaca, NY: Cornell University Press, 1998); W. Lance Bennett, "Social Movements beyond Borders: Understanding Two Eras of Transnational Activism," in *Transnational Protest and Global Activisim*, ed. Donatella della Porta and Sidney Tarrow (Lanham, MD: Rowman & Littlefield Publishing, 2005), 203-226; Donatella della Porta and Sidney Tarrow, "Transnational Processes and Social Activism: An Introduction," in in *Transnational Protest and Global Activisim*, ed. Donatella della Porta and Sidney Tarrow (Lanham, MD: Rowman & Littlefield Publishing, 2005), 1-17; Sidney Tarrow and Doug McAdam, "Scale Shift in Transnational Contention," in in *Transnational Protest and Global Activisim*, ed. Donatella della Porta and Sidney Tarrow (Lanham, MD: Rowman & Littlefield Publishing, 2005), 121-147; Ruth Reitan, *Global Activism* (New York: Routledge, 2007).

Electronic copy available at: https://ssrn.com/abstract=2734336

Cyberspace is a digital arena for social, political, economic and cultural interaction accessible to human experience through electronic devices (smartphones, computers, tablets) and that works based on three main layers: physical (fiber optic cables, backbones), logical (protocols, internet, web, applications) and informational (contents).[154]

Digital communication is a key aspect in the cyber domain for social, political, economic and cultural interactions. Digital communication systems, by definition, are communication systems that use a digital sequence as an interface between the source and the channel input (and similarly between the channel output and final destination). In cyberspace, digital communication process occurs through layers. For digital communication to happen there is needed:(1) symbolic features/ content (text, video, audio, digital identification etc.);(2) decoder / encoder device (computers, tablets, smartphones and others); (3) physical infrastructure for transporting and processing data (backbones, optical fiber); and (4) applications (software, web, protocols, blog, social media etc.).[155]

In order to understand how activists use digital communication it is important to identify first the main cyber effects on social practices, since transnational activism is embedded in social relations. Four main cyber effects on social practices are identified in this study: (1) Strengthening media connectivity, (2) Encouraging aggregation, (3) Increasing reality perception, and (4) Diffusing power.

Strengthening media connectivity involves the structure of permanent connectivity, in which individuals are now routinely connected to digital communication devices everywhere, all the time. Cyberspace has turned the ordinary citizen into one who carries an ubiquitous media device. The various types of devices are now so common they have faded into the background of everyday routine, and in that way become "invisible". It means that the tendency now is for the ordinary citizen to be connected full-time by means of omnipresent communication devices.[156]

Encouraging aggregation implies three concepts: long tail phenomenon, like-minded idea and emergent convergence culture.[157] Cyberspace amplifies the concentration of ideas, preferences and interests.[158] The individual now has the tool to find other groups or individuals who hold common ideas, and it condenses the convergence culture phenomenon – more important than the technological

[154] Michael Benedikt, "Cyberspace: Some Proposals," in *Cyberspace: First Steps*, ed. Michael Benedikt (Cambridge, MA: The MIT Press) 119-224; Stephen J. Kobrin, "Territoriality and the Governance of Cyberspace," *Journal of International Business Studies* 32 (2001): 687-704; Xiaoqing Shi and Hai Zhuge, "Cyber Physical Socio Ecology," *Concurrency and Computation: Practice and Experience* 23 (2010): 972-985, Published online 28 August 2010. DOI: 10.1002/cpe.1625; Nazli Choucri, Cyberpolitics in International Relations (Cambridge, MA: The MIT Press, 2012); Nazli Choucri and David Clark, "Integrating cyberspace and International Relations: The Co-Evolution Dilemma," MIT/Harvard ECIR Workshop on Who Controls Cyberspace? Cambridge, MA, November 6-7, 2012; Melissa E. Hathaway and Alexander Klimburg, "Preliminary Considerations: On National Cyber Security," in *National Cybersecurity: Framework Manuel*, ed. Alexander Klimburg (Tallinn: NATO Cooperative Cyber Defence Centre of Excellence), 1-43; Lucas Kello, "The Meaning of the Cyber Revolution," *International Security* 38 (2013): 7-40; Jan-Frederik Kremer and Benedikt Müller, " SAM: A Framework to Understand Emerging Challenges to States in an Interconnected World," in *Cyberspace and International Relations: Theory, Prospects and Challenges*, ed. Jan-Frederik Kremer and Benedikt Müller (Switzerland: Springer, 2014), 41-58.

[155] Robert G. Gallagher, *Principles of Digital Communication* (Cambridge: Cambridge University Press, 2008); David Clark, "An Insider's Guide to the Internet", *M.I.T. Computer Science and Artificial Intelligence Laboratory*. Version 2.0 7/25/04, 2004: http://groups.csail.mit.edu/ana/Publications/PubPDFs/An-Insiders-Guide-to-the-Internet.pdf.

[156] Reitan, Global Activism; Milton L. Mueller, *Networks and States* (Cambridge, MA: The MIT Press, 2010); Fabien Miard, "Call for power? Mobile phones as facilitators of politcal activism," in *Cyberspaces and Global Affairs,* ed. Sean S. Costigan and Jake Perry (Burlington, VT: Ashgate, 2012) 119-144; Philip Seib, *Real-time diplomacy: Politics and power in the social media era* (New York: Palgrave Macmillan, 2012); Bruce Bimber,, Andrew Flanagin, and Cynthia Stohl, *Collective Action in Organizations: Interaction and Engagement in an Era of Technological Change (*Cambridge: Cambridge University Press, 2012); José van Dijck, *The Culture of Connectivity: A Critical History of Social Media* (New York: Oxford University Press, 2013); Andreas Hepp and Friedrich Krotz, "Mediatized Worlds- Understanding Everyday Mediatization," in *Mediatized Worlds Culture and Society in a Media Age*, ed. Andreas Hepp and Friedrich Krotz (New York: Palgrave, 2014) 1-18.

[157] Chris Anderson, *The Long Tail: Why the Future of Business is Selling Less of More* (New York: Hyperion, 2006); Henry Jenkins, *Convergence Culture: Where Old and New Media Collide* (New York: New York University Press, 2008).

[158] Cass Sustein, *Republic.com* (Princeton, NJ: Princeton University Press, 2001); Seib, *Real-time diplomacy*; Choucri, *Cyberpolitics*.

Electronic copy available at: https://ssrn.com/abstract=2734336

convergence of multi-media devices is the convergence of ideas and interests that takes place in a symbolic environment created by digital communication. This convergence makes it possible to undertake concrete actions in the real world. Convergence culture is more than simply a technological shift and refers to a process, not an endpoint.[159]

Increasing reality perception means that virtuality blurs boundaries not only between online and offline, or public and private, but also between geographical distance and timing. The understanding of the world is no longer based only on formal filters (such as media, school and other traditional intermediaries), the new way to get information dilates individuals' worldview. The individual is exposed daily to a variety of ideas and compelled to think or give opinion on what appears on "screen". Cyberspace has expanded the worldview of individuals through receiving information from different sources, themes, places and levels of complexity.[160]

Diffusing power involves a new definition of power. Cyberpower is the ability to obtain preferred outcomes (*within* cyberspace or in other domains *outside* cyberspace) by using interconnected information through Internet, intranets, cellular technologies and space-based communications. These resources characterize the domain of cyberspace and are defined by infrastructure, location, networks, software, and human skills. In this context, power will increasingly be described by connections — who is connected to whom and for what purposes, therefore the measure of this power is connectedness. It is important to point out that distribution of power does not mean equality of power.[161]

Analysis of these four cyberspace effects on transnational activism's dynamic indicates that digital communication creates conditions that contribute to transnational activism's dynamic in different ways. The activism's dynamic is defined by six phases: Arrangement of the cause, individual engagement, action planning, execution of actions, visibility production and reaction or counter-attacks. Arrangement of the cause is when an activist idea is activated and delimited by a political cause, target or claim. Individual engagement is when the individual, after incorporating the activist cause and ideas, decides to engage and join the cause. Action planning is when a cause's supporters plan actions, collect information and decide guidelines and tactics. Execution of actions is when there is an action on behalf of the cause aiming at political results. Visibility production is when there is image management by the members. Reaction or counter-attacks is when defensive actions or counter-attacks happen.

---

[159] Jenkins, *Convergence Culture*.

[160] Shi and Zhuge, "Cyber Physical Socio Ecology," 972-985; Choucri, *Cyberpolitics*; Roxana Radu, "Power Technology and Powerful Technologies - Global Governmentality and Security in the Cyberspace," in *Cyberspace and International Relations: Theory, Prospects and Challenges*, ed. Jan-Frederik Kremer and Benedikt Müller (Switzerland: Springer, 2014) 3-21; James Miller, "Intensifying Mediatization: Everyware Media. Mediatized Worlds- Understanding Everyday Mediatization," in *Mediatized Worlds Culture and Society in a Media Age*, ed. Andreas Hepp and Friedrich Krotz (New York: Palgrave, 2014) 107-122.

[161] Madeline Carr, "A Political History of the Internet: A Theoretical Approach to the Implications for US Power," Conference Paper at the *International Studies Association Annual Meeting*, February 15-18, New York: 2009; Daniel Drezner, "Weighing the Scales: The Internet's Effect on State-Society Relations," *Borwn Journal of World Affairs* XVI (2010): 31-46; Joseph Nye, "Cyber Power," Paper from *Belfer Center for Science and International Affairs, Harvard Kennedy School* (May 2010); Kello, "The Meaning of the Cyber"; David P. Fidler, "authoritarian Leaders, the Internet, and Intenrational Politics," Journal of Diplomacy & International Relations 15 (2014): 7-21; Jeffrey A. Hart, "Information and Communications Technologies and Power," in *Cyberspaces and Global Affairs,* ed. Sean S. Costigan and Jake Perry (Burlington, VT: Ashgate, 2012) 203-214; Eddie Walsh, "Viewpoint: An alternative perspective on cyber anarchy for policy-makers," in in *Cyberspaces and Global Affairs,* ed. Sean S. Costigan and Jake Perry (Burlington, VT: Ashgate, 2012) 233-235; Seib, *Real-time diplomacy*.

Electronic copy available at: https://ssrn.com/abstract=2734336

These four main cyberspace effects on social practices directly influence these six stages of previously described, as show in figure 1:

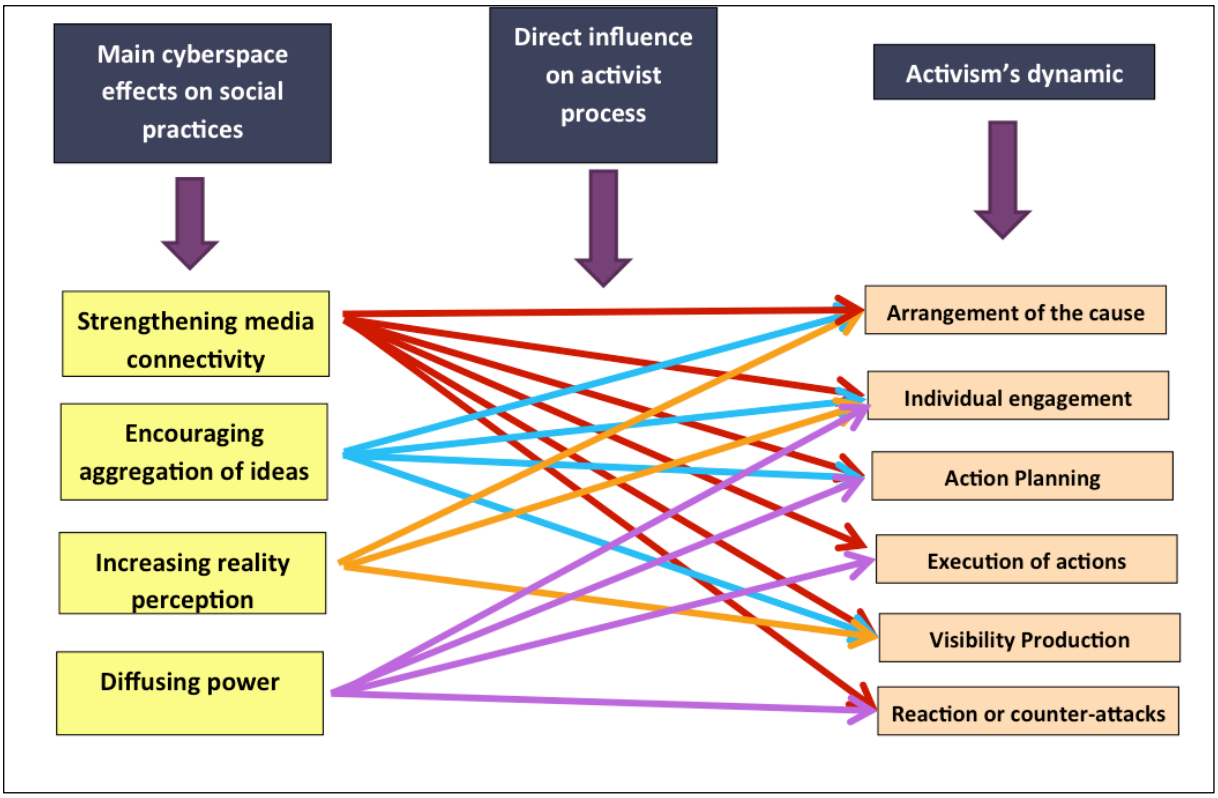


Figure 1:
Cyber effects on activism's dynamics

The main purpose of this diagram is to identify and assess how the cyber effects directly influence the activism's process. Therefore, it is possible to identify that digital communication:

1. **Enables** configuration of the cause
2. **Multiplies** individual engagement
3. **Equips** action planning
4. **Empowers** execution of actions
5. **Amplifies** visibility production
6. **Empowers** reaction or counter-attacks

This thus provides a useful perspective about contemporary transnational activism. To illustrate this point of view, this study examines each of the identifications above considering three emblematic cases: WikiLeaks, Arab Spring and Al Qaeda.

Digital communication enables configuration of the cause. Dispersed beliefs and claims can be turned into a cause through the convergence of ideas and interests within cyberspace. Digital communication catalyzed the uprisings in the Arab region; discontent about social and political injustices was compounded by decades of institutional and political decay in that region. This collective sentiment then enabled the process for the riots and demonstrations. In December 2010, the

Electronic copy available at: https://ssrn.com/abstract=2734336

self-immolation of Mohamed Bouazizi was shocking to Tunisians' eyes, the Arab people and the rest of the world. A street vendor of fruits and vegetables, at 26, he had his products confiscated by government authorities in Tunisia because they considered his activity illegal. After petitioning for the return of his belongings in the administration headquarters and seeing his request denied, he threw flammable liquid on his own body and burned. Bouazizi was rescued and taken to hospital but died two weeks later on January 5, 2011. The strong image of Bouzazizi and his narrative circulated through social media and it set off protests in Tunisia. This emblematic fact culminated with the fall of President Ben Ali after two decades in power.

Digital communication multiplies individual engagement. Through digital communication, the individual has access to new possibilities for engagement, including different types and degrees of effort in support of causes. This is related to online mobilization, recruitment, and online efforts to move people to action, protest, intervene, advocate and/or support a political cause. In the case of Al Qaeda, there is a global support base which is highly skilled at using computers and internet; and 80% of terrorist recruitment is through the internet.[162] This terrorist group has a global fundraising network that is based on a foundation of charities, nongovernmental organizations and other financial institutions, that solicit and gather funds through Web sites (for example via PayPal), Internet based chat rooms and forums. The practice of criminal activity is also part of the alternatives to raise funds by terrorists.

Digital communication equips action planning. Activists have greater ability to gather information, evaluate scenarios, and design tactics. About 50% of the protesters in Egypt (2010/2011) used Facebook and 13% used Twitter to communicate about the protest. The online magazine Al Battar, published by activists linked to al-Qaeda, contains detailed information about how to kidnap relevant people from the political and economic field, how to shoot grenades, and other related tutorials. This magazine has developed a true virtual training camp.[163] Al Qaeda operatives relied heavily on the Internet in planning and coordinating the September 11th attacks. Thousands of encrypted messages that had been posted in a password-protected area of a website were found by federal officials on the computer of arrested al Qaeda terrorist Abu Zubaydah, who reportedly masterminded the September 11th attacks. The first messages found on Zubaydah's computer were dated May 2001, and the last were sent on September 9, 2001. The frequency of the messages was highest in August 2001. To preserve their anonymity, the al Qaeda terrorists used the Internet in public places and sent messages via public e-mail. Some of the September 11th hijackers communicated using free web-based e-mail accounts.

Digital communication empowers execution of actions. Activist groups have more tools available to accomplish their goals, including cyberspace, as a new arena for disputes and attacks. In 2010 WikiLeaks had 40 core volunteers and about 800 mostly unpaid followers to maintain a diffuse web of computer servers with published data and an encrypted system for receiving information leaked anonymously. The possibility of obtaining classified documents through digital copies has empowered activists. The distribution via the Internet also gives more power to the group, affecting governments around the world.

[162] Ellen Hallams, "Digital diplomacy: the internet, the battle for ideas & US foreign policy," *CEU Political Science Journal* 5 (2013): 538-574.
[163] Hallams, "Digital diplomacy".

Electronic copy available at: https://ssrn.com/abstract=2734336

Digital communication amplifies visibility production. Activists can better manage their image and identity without traditional gatekeepers (even though the traditional media can participate in the diffusion process) and can disseminate narratives that tell their stories, ideas and actions. Research shows that during the Arab Spring protests in Egypt, about 50% of the demonstrators produced and disseminated videos or images of political protests in the streets, especially through Facebook.[164] The growth of jihadist sites over time shows the jump of only two sites in 1998 to over 4,700 in 2005. Currently in operation are 5,000 to 10,000 radical websites.[165]

Digital communication empowers reaction or counter-attacks. Activists are able to use new instruments/tools to defend themselves from attacks or to conduct counter-attacks. After the release of State Department cables in November 2010 by WikiLeaks, Amazon stopped acting as a host for WikiLeaks' material; the firm that managed WikiLeaks' domain name, EveryDNS.net, suspended its services, so that the domain name wikileaks.org was no longer operable; and PayPal stopped accepting donations for Mr. Assange's group. These and others business decisions hurt WikiLeaks significantly. Assange called it 'economic censorship' and claimed that actions by these financial intermediaries cost WikiLeaks three-quarters of a million dollars in lost donations. For this reason, hackers (especially Anonymous group) concatenated invasions of websites of several companies and businesses (like PayPal, Amazon, Visa.com) to retaliate with denial of service attacks against several of the firms that severed ties with WikiLeaks, making them inaccessible or slow. In the case of the Arab Spring process, turning off the internet by the Egyptian regime from the 25th of January to the 2nd February, 2011 caused the opposite effect to that provided by the authority. First, a small group, but with vast knowledge of information technology, continued to send information and videos to the outside about what was happening in Tahrir Square. Second, the fact that people no longer had access to the internet, caused greater interest in what was happening in their country, so that encouraged people to go to the streets, intensifying the protests.

[164] Zeynep Tufekci and Christopher Wilson, "Social Media and the Decision to Participate in Political Protest: Observations from Tahrir Square," *Journal of Communication* 62 (2012): 363-379.
[165] Hallams, "Digital diplomacy".

Electronic copy available at: https://ssrn.com/abstract=2734336

References

Anderson, Chris. 2006. *The Long Tail: Why the Future of Business is Selling Less of More*. New York: Hyperion.

Benedikt, Michael. 1991. Cyberspace: Some Proposals. In: *Cyberspace: First Steps*, ed. Michael Benedikt, 119-224, Cambridge, MA: The MIT Press.

Bennett, W. Lance. 2005. Social Movements beyond Borders: Understanding Two Eras of Transnational Activism. In *Transnational Protest and Global Activism,* ed. Donatella della Porta and Sidney Tarrow, 203-226, Lanham, MD: Rowman & Littlefield Publishing.

Bimber, Bruce, Andrew Flanagin, and Cynthia Stohl. 2012. *Collective Action in Organizations: Interaction and Engagement in an Era of Technological Change*. Cambridge: Cambridge University Press.

Carr, Madeline. 2009. A Political History of the Internet: A Theoretical Approach to the Implications for US Power. Conference Paper. February 15-18, New York. International Studies Association Annual Meeting.

Choucri, Nazli. 2012. *Cyberpolitics in International Relations*. Cambridge, MA: The MIT Press.

Choucri, Nazli and David Clark. 2012. Integrating Cyberspace and International Relations: The Co-Evolution Dilemma. MIT/Harvard ECIR Workshop on Who Controls Cyberspace? Cambridge, MA, November 6-7.

Clark, David. 2004. An Insider's Guide to the Internet. M.I.T. Computer Science and Artificial Intelligence Laboratory. Version 2.0 7/25/04. http://groups.csail.mit.edu/ana/Publications/PubPDFs/An-Insiders-Guide-to-the-Internet.pdf

Drezner, Daniel W. 2010. Weighing the Scales: The Internet's Effect on State-Society Relations. *Brown Journal of World Affairs* XVI (Spring/Summer): 31-46.

Fidler, David P. 2014. Authoritarian Leaders, the Internet, and International Politics. *Journal of Diplomacy & International Relations* 15 (Fall/Winter): 7-21.

Gallager, Robert G. 2008. *Principles of Digital Communication*. Cambridge: Cambridge University Press.

Hallams, Ellen. 2013. Digital diplomacy: the internet, the battle for ideas & US foreign policy. *CEU Political Science Journal* 5 (4): 538-574.

Hart, Jeffrey A. 2012. Information and Communications Technologies and Power. In *Cyberspaces and Global Affairs,* ed. Sean S. Costigan and Jake Perry, 203-214, Burlington, VT: Ashgate.

Electronic copy available at: https://ssrn.com/abstract=2734336

Hathaway, Melissa E., and Alexander Klimburg. 2012. Preliminary Considerations: On National Cyber Security. In *National Cybersecurity: Framework Manual*, ed. Alexander Klimburg, 1-43, Tallinn: NATO Cooperative Cyber Defence Centre of Excellence.

Hepp, Andreas and Friedrich Krotz. 2014. Mediatized Worlds- Understanding Everyday Mediatization. In *Mediatized Worlds Culture and Society in a Media Age*, ed. Andreas Hepp and Friedrich Krotz, 1-18, New York: Palgrave.

Jenkins, Henry. 2008. *Convergence Culture: Where Old and New Media Collide*. New York: New York University Press.

Keck, Margaret E. and Kathryn Sikkink. 1998. *Activists beyond Borders: Advocacy Networks in International Politics*. Ithaca, NY: Cornell University Press.

Kello, Lucas. 2013. The Meaning of the Cyber Revolution. *International Security* 38 (Fall): 7-40.

Kobrin, Stephen J. 2001. Territoriality and the Governance of Cyberspace. *Journal of International Business Studies* 32 (4): 687-704.

Kremer, Jan-Frederik and Benedikt Müller. 2014. SAM: A Framework to Understand Emerging Challenges to States in an Interconnected World. In *Cyberspace and International Relations: Theory, Prospects and Challenges*, ed. Jan-Frederik Kremer and Benedikt Müller, 41-58. Switzerland: Springer.

Miard, Fabien. 2012. Call for power? Mobile phones as facilitators of politcal activism. In *Cyberspaces and Global Affairs,* ed. Sean S. Costigan and Jake Perry, 119-144, Burlington, VT: Ashgate.

Miller, James. 2014. Intensifying Mediatization: Everyware Media. Mediatized Worlds- Understanding Everyday Mediatization. In *Mediatized Worlds Culture and Society in a Media Age*, ed. Andreas Hepp and Friedrich Krotz, 107-122, New York: Palgrave.

Mueller, Milton L. 2010. *Networks and States.* Cambridge, MA: MIT Press.

Nye, Joseph. 2010. Cyber Power. Paper. Belfer Center for Science and International Affairs, Harvard Kennedy School. May.

Porta, Donatella della and Sidney Tarrow. 2005. Transnational Processes and Social Activism: An Introduction. In *Transnational Protest and Global Activism,* ed. Donatella della Porta and Sidney Tarrow, 1-17, Lanham, MD: Rowman & Littlefield Publishing.

Radu, Roxana. 2014. Power Technology and Powerful Technologies - Global Governmentality and Security in the Cyberspace. In *Cyberspace and International Relations: Theory, Prospects and Challenges*, ed. Jan-Frederik Kremer and Benedikt Müller, 3-21. Switzerland: Springer.

Electronic copy available at: https://ssrn.com/abstract=2734336

Reitan, Ruth. 2007. *Global Activism*. New York: Routledge.

Seib, Philip. 2012. *Real-time diplomacy: Politics and power in the social media era*. New York: Palgrave Macmillan.

Shi, Xiaoqing and Hai Zhuge. 2010. Cyber Physical Socio Ecology. *Concurrency And Computation: Practice and Experience* 23 (9): 972-985. Published online 28 August 2010. DOI: 10.1002/cpe.1625.

Slaughter, Anne-Marie. 2009. America's Edge: Power in the Networked Century. *Foreign Affairs* 88 (January/February): 94-113.

Sustein, Cass. 2001. *Republic.com*. Princeton, NJ: Princeton University Press.

Tarrow, Sidney, and Doug Mcadam. 2005. Scale Shift in Transnational Contention. In *Transnational protest and Global Activism,* ed. Donatella della Porta and Sidney Tarrow, 121-147, Lanham, MD: Rowman & Littlefield Publishing.

Tufekci, Zeynep and Christopher Wilson. 2012. Social Media and the Decision to Participate in Political Protest: Observations From Tahrir Square. *Journal of Communication* 62 (14): 363–379.

Van Dijck, José. 2013. *The Culture of Connectivity: A Critical History of Social Media*. New York: Oxford University Press.

Walsh, Eddi. 2012. Viewpoint: An alternative perspective on cyber anarchy for policy-makers. In *Cyberspaces and Global Affair*s, ed. Sean Costigan and Jake Perry, 233-235, Burlington, VT: Ashgate.

Electronic copy available at: https://ssrn.com/abstract=2734336