MIT
POLITICAL SCIENCE

Massachusetts Institute of Technology
Political Science Department

Research Paper No. 2016-2

Perspectives on Cybersecurity:
A Collaborative Study

Massachusetts Institute of Technology:

Nazli Choucri
Chrisma Jackson
Lyla Fischer
Brooke Gier
Vivian Peron
Ben Ze Yuan
Liu Yangyue
Glenn Voelz

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

Table of Contents

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

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?

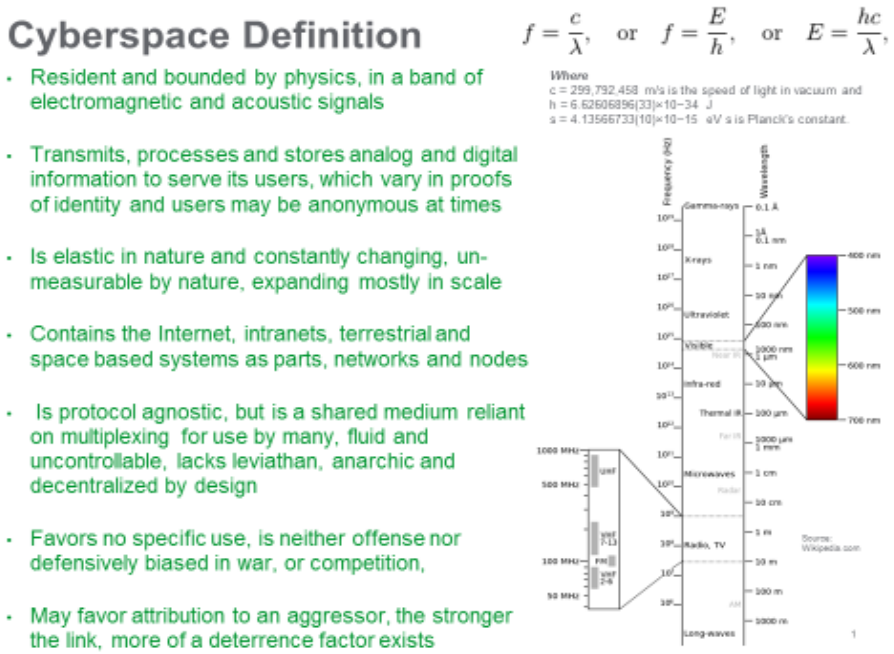

Figure 1.1
Source: George Wren. MIT Cybersecurity Seminar, Spring 2015.

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?

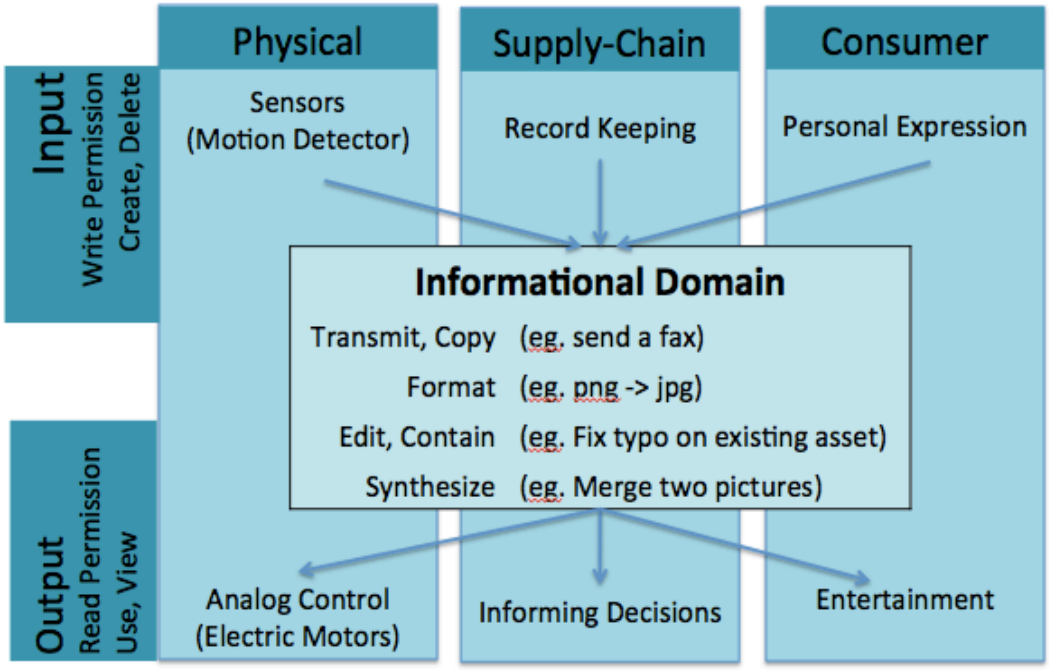

Figure 1.2
Source Lyla Fisher, MIT Cybersecurity Seminar, 2015.

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

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

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

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.