Chapter 106
Motivating Cybersecurity:
Assessing the Status of Critical Infrastructure as an Object of Cyber Threats

Sean Lawson
University of Utah, USA

ABSTRACT

Based on an analysis of key policy documents and statements from civilian policymakers, military leaders, and cybersecurity experts, this chapter demonstrates that although there is still concern over cyber threats to critical infrastructure, other threat objects have begun to figure more prominently in public policy discourse about cybersecurity in the United States. In particular, intellectual property and government secrets are now identified most often as the primary object of cyber threats. When critical infrastructure is mentioned, it is often used as a motivational tactic, with collapse of critical infrastructure serving as a central theme of hypothetical scenarios meant to motivate a policy response. This chapter documents and critically evaluates this shift in U.S. cybersecurity discourse.

INTRODUCTION

As advanced Western societies and economies have become increasingly dependent upon networked information and communication systems, concern over the security and reliability of those systems has also increased. This concern with cybersecurity has gone hand-in-hand with increased concern about the security and reliability of critical infrastructures. For most of the 1990s and early 2000s, cybersecurity experts, military leaders, and policymakers in the United States identified critical infrastructure as the primary object of prospective cyber threats either from state or non-state actors. While public policy discussion of cybersecurity in the United States waned during the wars in Afghanistan and Iraq, a number of well-publicized cyber attacks since 2007 against Estonia, Georgia, and Iran have focused attention once again on cybersecurity. In the process, however, critical infrastructure has slipped from its position as the primary object of the cyber threat. Although there is certainly still concern over cyber threats to critical infrastructure,

DOI: 10.4018/978-1-4666-5942-1.ch106

other threat objects have begun to figure more prominently in public policy discourse about cybersecurity in the United States. In particular, intellectual property and government secrets are now identified most often as the primary object of cyber threats. When critical infrastructure is mentioned, it is often used as a motivational tactic, with collapse of critical infrastructure serving as a central theme of hypothetical scenarios meant to motivate a policy response. This chapter documents and critically evaluates this shift in the U.S. cybersecurity discourse by analyzing a collection of significant policy documents and public statements from policymakers, military leaders, and cybersecurity experts.

The next section of this chapter explains the sources that were examined for this study, as well as the theories and methods used to analyze those sources. The bulk of the chapter addresses the past and present status of critical infrastructure as an object of concern in the ongoing U.S. public policy debate about cybersecurity. In particular, it demonstrates that, since 2009, significant policy documents, as well as statements from military leaders, policymakers, and cybersecurity experts in the United States, most often identify private intellectual property, government secrets, and the economy as the primary objects of cyber threats. It also examines the status of critical infrastructure as an object of cyber threats in these same documents and statements. The final section of this chapter identifies potentially negative impacts of this shift in U.S. cybersecurity discourse and provides suggestions for how these can be overcome.

BACKGROUND

This chapter is informed by the results of an ongoing research project that is monitoring, documenting, and analyzing the evolving public policy discourse about cybersecurity in the United States. Previous studies of U.S. cybersecurity discourse (discussed in more detail below) have noted that perceptions of cyber threats have changed over time. With renewed interest in cybersecurity coinciding with several well-publicized cyber attacks and the election of a new president in the United States, this project has worked to determine the degree to which dominant perceptions of cyber threats may have changed across a number key categories. This chapter focuses on the relationship of critical infrastructure to two of those categories: the object and impact of cyber threats.

This chapter is based on an analysis of what have been called "discourse events." Discourse events are documents or statements that are reflective of or have the power to shape the overall public policy debate about cybersecurity in the United States. While there are thousands of news stories, blog posts, discussion forum posts, and more each week about cybersecurity, these are not necessarily representative of dominant perceptions of cyber threats, and very few have the power to shape the overall discussion of the issue. They do not count as discourse events. Discourse events are produced by high-ranking policymakers, military leaders, Internet security companies, security experts, or veteran journalists and include accounts from influential media sources, government policy documents, industry and think-tank reports, military strategy and doctrine publications, and speeches, op-eds, or Congressional testimony by civilian policymakers, military leaders, or experts. This chapter is informed by the collection and analysis of over one hundred such documents since 2009.

The analysis of these documents has been shaped by the critical constructivist tradition of scholarship in security studies (Peoples and Vaughan-Williams, 2010), and in particular the body of scholarship that has examined the role of language, discourse, and perception in identifications of and responses to cyber threats (Bendrath, 2001, 2003; Dunn Cavelty, 2008; Eriksson, 2002; Hansen & Nissenbaum, 2009). Drawing heavily from "securitization theory," this work begins with the observation that it is not predetermined which security threats will