Chapter V
Infrastructures of Cyber Warfare

Robert S. Owen
Texas A&M University, USA

ABSTRACT

Discussions of cyber warfare tend to focus on weakening or disrupting a physical critical core infrastructure. Critical infrastructures are systems and assets that if destroyed, would have an impact on physical security, economic security, and/or public health or safety. Some have argued that meaningful, sustainable damage to critical infrastructures is unlikely through cyber warfare tactics. However, damage to non-critical infrastructures could inflict considerable economic damage and could cause an existing or emerging technology to lose acceptance in a targeted region or society. War planners with goals of economic damage or decreased quality of life could achieve these ends at relatively low cost without attempts to physically attack the critical infrastructure itself. Much of the work to carry out attacks on non-critical infrastructures could be done by a worldwide network of volunteers who might not even be aware of the motivations of the war planners or cyber terrorists. Non-critical infrastructures that are vulnerable to damage are outlined and discussed. Greater concern for and attention to the vulnerabilities of these non-critical infrastructures is advocated.

INTRODUCTION

This chapter makes an appeal for greater attention to non-critical infrastructures that are vulnerable to cyber warfare. Cyber warfare discussions sometimes debate the extent of damage that can or cannot be caused to a critical infrastructure or if the infrastructure is even vulnerable. The focus of these discussions tends to presume a focus on weakening or disrupting a critical core infrastructure of some sort, such clogging the bandwidth of an Internet connection or crashing a server in the case of the Internet infrastructure. Evidence, however, seems to suggest that it is unlikely that cyber terrorists or other war planners could cause meaningful damage to critical infrastructures through cyber warfare tactics (Lewis, 2003).

Additional non-critical infrastructures are proposed here as necessary to the diffusion and continued use of a technology: customer infrastructures that include a social infrastructure and a commercial infrastructure, and a political/regulatory infrastructure that moderates the customer infrastructures. Tactics

that target these accompanying infrastructures could be part of a larger strategy to disrupt the core technological or physical infrastructure in order to cause economic damage or a decrease in quality of life. Although such tactics are not likely to be useful for immediate mass destruction of a technology or associated physical infrastructure, they could be effective in blocking the diffusion of an emerging technology or of causing an existing technology to lose acceptance in a targeted region or society.

BACKGROUND

Discussions of "cyber terrorism" tend to work from a definition something like:

The use of computer network tools to shut down critical infrastructures for the purpose of coercing or intimidating a government or civilian population. (cf., Caruso, 2002; Lewis, 2002)

"Critical infrastructures" are systems and assets that if destroyed, would have an impact on physical security, national economic security, and/or national public health or safety (HR 3162, 2001) and includes such industries or operations as (to name only a few) energy, food, transportation, banking, communication, government, and cyberspace itself (cf., DHS, 2003a, 2003b). "Cyberspace" refers to the interconnected computers, servers, routers, switches, and cables that make critical infrastructures work (cf., DHS, 2003a).

Although the sudden debilitating failure of some critical piece of the cyberspace infrastructure might be an objective of terrorism, the impact of smaller incidents that could be used by cyber warfare strategists to merely temporarily "cripple" critical infrastructures are perhaps more possible and more likely, and, in aggregate, are perhaps much more costly overall. Failures of critical infrastructures occur naturally in ordinary every day life, causing power outages, flight delays, and communication disruptions, and societies that depend on these critical infrastructures seem to be resilient to these events; cyber attacks on these critical infrastructures are likely to be less effective than nature (cf., Lewis, 2002).

The perspective of the article is that while a digital 9/11 is unlikely, smaller, perhaps individually insignificant, incidents can serve two useful strategic functions: they can erode public confidence in systems that rely on cyberspace, and they can be used by cyberwar planners to prepare for future attacks. In preparing for later attacks, cyberwar planners can map information systems, identify key targets, and lace an infrastructure with "back doors" that create future points of entry (DHS, 2003a). Of greater interest in the present chapter, erosion of public confidence in a system is likely to cause less reliance on that system; decreased use of a system due to lack of confidence is in many ways the same end result as if a part of the system had been destroyed by a single huge attack. The primary difference is that a huge attack on a critical infrastructure might be impossible to implement; many seemingly insignificant attacks, on the other hand, could be easily implemented at low cost.

This chapter proposes that infrastructures other than critical core infrastructures are vulnerable, important, and deserving of greater attention. A gang of thugs does not have to blow the foundation out from under the house to force a resident out of the neighborhood. Giving candy to neighborhood children to throw rocks whenever the windows are replaced could be every bit as effective. From that perspective—that an important asset can be easy to cripple with a thousand stones even though impossible to kill with a single boulder—the goal of the present chapter is to propose infrustructures that might be associated with critical infrastructure vulnerability. In addition to a critical core infrastructure—servers, routers, switches, cables, and such in the case of the Internet—this article proposes that we conceptually consider a social infrastructure, a commercial infrastructure, and a political/regulatory infrastructure in devising strategies to defend against cyber warfare.