PacNet
Number 81

Pacific Forum CSIS
Honolulu, Hawaii

Dec. 3, 2012

What Happens when Critical Infrastructure Defenses Fail? by Clete DiGiovanni and David Hamon

Dr. Clete DiGiovanni (cdig@cox.net) is a retired Medical & Public Health Advisor in the Advanced Systems and Concepts Office of the Defense Threat Reduction Agency. Mr. David Hamon (david.hamon@anser.org) serves as Distinguished Analyst and Director with Analytic Services, Inc., and is a Pacific Forum Non-Resident Senior Fellow.

Largely ignored in the public discussion of cyber sabotage has been the need for contingency planning should critical infrastructure defenses fail and community leaders suddenly have to manage and mitigate the consequences of a successful attack that disrupts electricity, banking, transportation, or other essential services.

This issue cuts across nationalities, territories, jurisdictions, and security interests. Moreover, given recent incidents in the Asia-Pacific region, there is every reason to believe that Hawaii, the US territories, and the Pacific Command area of operations (PACOM-AOR) are particularly vulnerable. Hawaii, Guam, and other US territories have military facilities and dependent populations that may be subject to such attacks.

Even in technologically advanced countries, critical infrastructure defenses are susceptible to penetration because of the rapid evolution of hackers' capabilities. Take, for example, what recently happened to Japan, our key Asian ally and trusted security partner.

On September 13, China's largest hacker group posted on its website a "declaration of war" against Japan in a dispute over the ownership of five islands in the East China Sea. Targeted were approximately 300 websites of local and national government agencies, schools, universities, banks, electric companies, an airline, and other public and private sector entities. According to a compilation of these incidents made available by Hitachi Systems, Ltd., attacks consisted of web defacements and denials of services. Websites became unusable for periods ranging from a few hours to two weeks or longer. The Supreme Court's site was shut down on September 14 and did not become fully available until September 28; searching judicial precedents was impossible during this time. Soon after these attacks began, the Minister of Internal Affairs and Communications stated that, ". . . Japan is now under cyber-attacks and (the consequences of these attacks) are alarming."

The US also recently experienced an attack on a sector of its critical infrastructure. At the end of September, a Middle Eastern group flooded the websites of six major US banks with such a volume of messages that the banks' clients were unable to get timely access to their accounts to pay bills and conduct other transactions. Who did this and for what reason are currently being investigated. The banks were unable to prevent or promptly curtail these attacks, despite having been warned of them in advance. These attacks resumed in mid-October.

A Congressional Research Office report issued in April 2004 and just re-issued warned of the vulnerability of America's electric power grid to cyber attacks. Although no successful attack against our grid has yet occurred, McAfee, an internet security firm, in a July report noted that, "The most prevalent cyber threat reported by the global energy sector is extortion. Criminals gain access to a utility's system, demonstrate that they are capable of doing damage, and demand a ransom . . . one in four power companies globally said that they had been victims of extortion."

Criminals are not the only perpetrators of this activity. Agents of nation states masking their identities have both the means and motivation for carrying out such attacks.

Advances in malicious code-writing can now result in physical destruction of a target. In a controlled experiment in 2007, workers at the Idaho National Laboratory wrote cyber commands that resulted in self-destruction of a power generator. Two years later, the Stuxnet virus was released that eventually infected the systems that monitor and manage Iran's nuclear processing centrifuges and destroyed many of them. Earlier this year, as Defense Secretary Leon Panetta recently revealed to the public, a virus named Shamoon "rendered useless" 30,000 computers of Saudi Arabia's state oil company. To be sure, the viruses that destroyed these centrifuges and computers were complicated codes, but it is risky to assume similar codes won't be written by other determined and well-funded state or non-state hackers. The expanding use of smart grid technology by US electric companies to increase their efficiency and profits also increases their vulnerability to such cyber threats because of the lack of security features consistently built into this technology, according to a July report issued by the US Government Accountability Office.

Improving and increasing our defenses is essential. But also essential is planning for the consequences of their failure.

Hindering that planning is incomplete understanding of how these failures would play out – what would be their scope and likely duration. We are dependent on the private sector for this understanding because our infrastructure is privately owned. Current efforts by the federal government and the private sector to improve communication between all parties about system vulnerabilities should also include detailed discussions about potential system failures and their consequences, especially if cyber-attacks disable equipment that is impossible to repair and difficult to replace promptly.

Discussing the consequences of systems failing because of inadequate defenses will be awkward for the stewards of those systems. But without this realistic and comprehensive understanding of the risks communities may face, contingency planning is impossible.

PacNet commentaries and responses represent the views of the respective authors. Alternative viewpoints are always welcomed.