

Cyber Threat to Critical Infrastructure - 2010-2015

Peter D. Gasper

September 2008

Prepared for presentation at:

Information & Cyberspace Symposium
Fort Leavenworth, Kansas
22-24 September 2008



Cyber Threat to Critical Infrastructure 2010-1015

A Word about Threat Assessment at INL

“Threat” is commonly, although not consistently, defined as: **Threat = Capability + Intent + Opportunity**. From the analytic perspective, the definition assumes the existence of a threat “source” – an actor or agent posing the threat. For many reasons, the vulnerability assessment process is developing at a faster pace than the threat assessment process. While vulnerability assessment aids in estimating the **Capability** factor in the Threat Equation, satisfactory assessment of **Intent** and **Opportunity** is more difficult.

The primary focus of cyber threats to critical infrastructure (CI) is on Control Systems (CS). These systems consist of a set of hardware and software acting in concert that gathers information and then performs physical functions based on established parameters and/or information it received.¹ The United States Computer Emergency Readiness Team (US-CERT) states that cyber threats to a CS refer to persons who attempt unauthorized access to a CS device and/or network using a data communications pathway. US-CERT also notes that threats to CS can come from numerous sources (e.g.

¹ The document *Department of Homeland Security: Cyber Security Procurement Language for Control Systems, August 2008* describes Control Systems (CS) as: Supervisory Control and Data Acquisition (SCADA), Process Control System (PCS), Distributed Control System (DCS), etc. CS generally refer to the systems which control, monitor, and manage the nation’s critical infrastructures such as electric power generators, subway systems, dams, telecommunication systems, natural gas pipelines, and many others.

national governments, terrorists, industrial spies, organized crime groups, hacktivists, and hackers).²

The Idaho National Laboratory (INL) is at the forefront of efforts to identify vulnerabilities to CS and provides assessments on potential capabilities malicious actors may seek to exploit those vulnerabilities. INL has a comprehensive array of research facilities to include the: SCADA Test Bed, Power Grid Test Bed, Mock Chemical Mixing Facility, Wireless Test Bed, and Physical Security Test Bed. Research conducted in these facilities provides practical, hands-on experience with all types of CS employed in critical infrastructure. Additionally, INL's extensive background in the study of existing and conceptual attack techniques enables INL to characterize how a threat source would "create" a **Threat** by developing a **Capability**. On a daily basis, the results of INL CS analysis are provided to the US-CERT in support of the DHS Control Systems Security Program (CSSP). INL, the Department of Energy (DoE), and vendors from private industry, work together to mitigate CS vulnerabilities along with elements of the Department of Defense and other U.S. agencies and services.

Trends in Critical Infrastructure (CI) Control Systems (CS)

Although a dramatic technological leap forward in CS in the CI environment is not forecast for the period 2010-2015, trends in key CS technologies must be noted. Viewed together, these trends indicate the future operational environment will be populated with

² US-CERT categorizes deliberate threats consistent with the remarks in the Statement for the Record to the Joint Economic Committee by Lawrence K. Gershwin, the Central Intelligence Agency's National Intelligence Officer for Science and Technology, 21 June 2001.

more CS in the CI sector, and those systems will have more communications elements. Thus, the CS impact on the future operational environment will be increased presence and exposure to threat sources.

Trend 1 - Proliferation of Control Systems: In nearly all sectors of critical infrastructure there is a move towards advanced automation using CS. For example, according to research from ARC Advisory Group the worldwide market for SCADA systems for the oil and gas industry is expected to grow at a compounded annual growth rate (CAGR) of 8.9% over the next five years.³

Trend 2 – Increased Digital and IP Base: CI CS networks are digital and Internet Protocol (IP) based - even those CS that rely solely on the “plain old telephone systems” (POTS) have digital components. In addition, on top of the general digital/IP base runs a profusion of different CS protocols. For example, manufacturers of intelligent electronic devices (IED) used in CS base their products on proprietary protocols, causing a significant confusion among the utilities about the types of protocols.⁴ While there are efforts to standardize protocols, the number of protocols in use continues to grow. From the CS protection perspective, the proliferation of protocols leads to a wider field of potential vulnerabilities.

Trend 3 - Expanded Use of Wireless Communications: According the ARC Advisory Group, the market for wireless technology in process manufacturing applications reached \$281 million in 2007. By the year 2012, the market is expected to grow to approximately

³ ARC: *SCADA Systems Market for Oil, Gas Industry to Reach \$1,141M*, July 6, 2007, URL: <http://petrochemical.ihs.com/news-07Q3/arc-scada-gas.jsp>

⁴ *Global Developments in Substation Automation (Technical Insights)*, Frost & Sullivan Research Service, June 28, 2006, URL: www.frost.com/prod/servlet/report-brochure.pag?id=D646-01-00-00-00

\$1.1 billion, a compound annual growth rate of 31.8%.⁵ This striking growth trend highlights already existing concerns over the security of many modes of wireless communications paths developed for CS. An illustration of one of these concerns is the layering of multiple access points (meshed wireless networks) for the advanced metering infrastructure (AMI), which provides the basis of many smart grid applications. With the increase of multiple radio frequency (RF) access points comes increased vulnerability to network penetration and CS exploitation. Thus, the new operational environment will be expanded to include RF access points ranging from globe-spanning satellite links to short range Bluetooth applications.

Trend 4 – Impediments to Security Measure Implementation: In addition to CS growth and proliferation trends, there is the trend to improve CS security. While many successful initiatives to introduce security systems and mitigate known vulnerabilities occur, other security programs are impeded by economic and organizational factors. For example, an effort has been made to reduce the potential for cascading power outages by systematic isolation of interconnected power grids using a concept known as “islanding.” Unfortunately, implementation of this security measure is behind schedule. Consequently, the operational environment of the period 2010-2015, with all of its increased presence and exposure of CS, will possess a national power grid still vulnerable to massive cascading power outages.

Implications of Technology Transfer

⁵ *Wireless in Process Manufacturing Worldwide Outlook – Market Analysis and Forecast through 2012*, ARC Advisory Group, 2008

Before the 1960s, control systems were in their infancy. Industrial processes and utilities were managed and monitored by humans. The development and production of CS were confined to the industrialized world, primarily the United States. In the ensuing forty plus years, newly industrialized nations emerged and CS technology quickly spread. Not only did foreign industries embrace the use of CS technology, some countries such as the People's Republic of China (PRC) became licensed producers of many components used in advanced CS. In the operational environment of 2010-2015, the CS and critical infrastructure of the new industrial nations will constitute a significant part of the CS presence and will share in the risks inherent in CS exposure. Furthermore, should one or more of the new producers of CS components desire to develop an anti-CS cyber capability, they have first-hand understanding of the latest CS technologies.

Increasing Interest in Control Systems Vulnerabilities

DEFCON-15, a so-called “underground hacker convention,” was held in Las Vegas during August, 2007. One session presented by Ganesh Devarajan dealt with SCADA system vulnerabilities which made a strong impression on many attendees. One attendee noted, “SCADA systems, the systems that run critical infrastructure such as water treatment plants, electrical grids and nuclear power plants have an overwhelming number of vulnerabilities. Scary. Nationwide emergency alert systems also have relatively easy attack vectors.”⁶ The impact of the presentation was not confined to the United States. Reports of the presentation quickly spread throughout the Internet, appearing even in Chinese and Russian language blogs and network security Web sites.

⁶ *Things I learned at DEFCON 15*, August 6, 2007, URL: <http://chainlynx.blogspot.com/2007/08/things-i-learned-at-defcon-15.html>

Since then, the chatter about SCADA and CS vulnerabilities in various forums accessed by suspected threat actors has increased significantly. Consequently, as the 2010-2015 period approaches, it can be anticipated that interested threat sources will employ some segment of their time and talents developing anti-CS exploits.

Russo-Georgian Conflict – Did it Change the Environment?

The ongoing Russo-Georgian conflict presents itself as an interesting final point for discussion. The media “played-up” the notion that a significant, perhaps even history changing, event accompanied the initiation of the conflict – a “cyber attack” had been launched against Georgian Web sites and networks. Open media analysis was confused on many points and the true initiator/threat actor has not yet been reliably identified by technical evidence. Speculation, inference, and wishful thinking point to agents working for Russia as the culprits. Various blogs and commentators make comparisons with alleged Russian attacks on Estonia, and some even recall the 6th Network War of National Defense conducted against the U.S. by PRC hacktivists in April 2001. What the commentators have not discussed is what did not happen during any of these events. For the purpose of this paper, INL analysis of these events does not yet show any examples of CS exploits or activity.

While there was no overt evidence of anti-CS activity, it must be understood that digital media analysis (cyber forensics) has not kept pace with the profusion of attack technologies. Therefore, reliable evidence is increasingly difficult to gather. So, if asked if the operational environment in the period 2010-2015 will be any different, the answer

must be developed with a studied recognition of CS deployment trends, expanding technology transfer, and increased interest in CS vulnerabilities. With those elements in mind, a case could be made that future conflicts, especially those of greater scope than the Russo-Georgian episode, might contain an anti-CS component in addition to the more conventional distributed denial of services (DDoS) attacks seen in the past.

Even if an anti-CS element was not introduced into the cyber component of the conflict, the way in which DDoS attacks were delivered in the Russo-Georgian conflict opens up a new concern to critical infrastructure relying on CS networks. The threat actor implemented the DDoS attacks by means of command-and-controlled botnets.⁷ Due to the increased presence and exposure of CS networks, future cyber conflicts might include undetected hosting of botnets on U.S. based CS networks.

This raises a new possibility - the operational environment in the 2010-2015 period, could include the highly undesirable dilemma of U.S. critical infrastructure CS server, unknowingly hosting a botnet, being a source of attacks on other U.S. assets. In a sense, the threat source would have created a “cyber holy site” to provide the cover or “sanctuary” of a “US entity” to lengthen his period of malicious activity.

Conclusion

⁷ Short for “robot network” - A network of hijacked PCs that can be used either to launch more spam, or to participate in denial of service attacks (DoS) that target a website and bombard it with traffic until it crashes. From a single computer, a botnet can send thousands of spam messages in one day. URL: www.spywareremove.com/glossary/ and www.independent.co.uk/news/business/analysis-and-features/how-cyber-crime-went-professional-892882.html

The preceding discussion does not constitute a formal threat assessment. It merely presents a listing of trends affecting CS development and a number of factors requiring monitoring and research. On the other hand, this discussion does project that the operational environment in 2010-2015 will likely see an increase in **Capability** and **Opportunity** available to threat sources. Coupled with the broader presence and exposure of control systems, this suggests the future operational environment will be both more congested and more vulnerable. Should a threat actor emerge that has the **Intent** the equation **Threat = Capability + Intent + Opportunity** will be complete.