

Cyber Warfare's Threat to Critical National Infrastructure

Written By Jeffrey Bernstein

Published April 2009 in MIS-ASIA

Recently, news concerning the ongoing security compromise of the North American power grid via various breaches of computing infrastructure was distributed throughout news and media outlets worldwide. While not a new problem by any means, the issue warrants attention from the international public, commercial and government sector audiences.

The electronic computing environments that make up a country's infrastructure are often taken for granted. However, a disruption to only a single live production computer system can create cascading consequences across multiple sectors. For example, a computer breach that disrupts the distribution of electrical power across a region could lead to the forced shutdown of networked communications and controls within the transportation sector. Air traffic, road traffic and rail transportation might become affected as a direct result. By extension, subsequent disruption of emergency services would also occur.

Recent highly publicised cyber attacks on the republics of Estonia, Lithuania and Georgia are representative of the growing problem at hand. Because each country has a unique environment, cyber attacks will yield varying consequences from nation to nation. Georgia, for instance, was a relative latecomer to adopt Internet technologies. Because of this, the country's population of fewer than five million saw little effect beyond service denial to many of its government Web sites. Cyber attacks have far less impact on a country such as Georgia than they might on more Internet-dependent places such as Taiwan, South Korea, Singapore or the United States where vital services including government, transportation, power and banking depend on the Internet.

These increasingly frequent, sophisticated and targeted international cyber incidents involving denial of service, espionage, propaganda and information theft are driving governments to develop effective tactical and strategic cyber-warfare capabilities. While government military forces have been traditionally more equipped for warfare involving guns, tanks and missiles, almost all now recognise the need to adopt strategies to support success in this new electronic theatre of operations. Most countries, of course, deny that their cyber capabilities are involved with any of the higher-profile international cyber security events that we read about in the press almost daily. Regardless of the truth in these denials, the anonymous nature of the Internet provides plausible deniability for attack sources.

Mission statement

In the Americas, the current mission statement of the United States Air Force is to 'Fly, Fight and Win...in Air, Space and Cyberspace'. Similarly, in Eastern Asia, The People's Liberation Army (PLA) reportedly continues to mature its integrated network electronic warfare and space/counter-space capabilities.

China and the US are only two of the countries included in the rapidly expanding list of nations now racing to assemble arsenals of cyber-weaponry. In fact, it is well-documented and commonly accepted by the international security community that more than 140 countries are actively developing cyber-espionage and warfare capabilities. The common thinking for all is to facilitate increased superiority over an adversary.

CRITICAL DEFENCE

When it comes to the modern-day battleground, 'bits and bytes' now accompany the 'bullets and bombs' that have historically powered warfare. As multinational cyber arsenals continue to mature, international concerns over operational cyber 'espionage' and 'warfare' grow.

Perhaps most vulnerable to attack are the critical infrastructure and key resources that operate within any particular country. Critical infrastructure resources support the crucial services that generally serve as the supporting foundation for any society.

Cyber security protection

With the majority of global vital infrastructure operated by the commercial sectors, the issue of cyber security protection is weighing heavily on both industry and government. For example, in the US, 80 per cent of critical infrastructure is owned and operated by the commercial sectors.

Some critical infrastructure elements are so essential that their destruction, disruption or exploitation could have a debilitating impact on a country's national security or economic well-being.

While critical infrastructure categorisation varies from country to country, it usually includes some combination of the following sectors from industry and government;

- Government services
- Law enforcement, fire and emergency response
- Banking and financial services
- Transportation
- Power including electricity, oil and gas
- Public works including water and drainage
- Internet, media and telecommunications
- Agriculture and food supply
- Health

Many countries also categorise prominent public places, national monuments and high-profile events as critical infrastructure.

Power and utility sectors

One specific area of concern is in the power and utility sectors where Supervisory Control and Data Acquisition (SCADA) industrial control systems monitor, coordinate and control process. Within the enterprise, information technology systems typically have a lifecycle of five years or less allowing for enhancements designed to mitigate the latest known security threats. By comparison, many mission critical SCADA control systems have been in production for 15 years and sometimes longer. Unfortunately, many of these systems were originally architected with little to no concern for security. Because of this, Internet-exposed SCADA-based systems and the organisations that operate them remain highly vulnerable to Internet-borne threat.

A recent article from the North America-based Council on Foreign Relations quoted a well-known economist as having estimated that a shutdown of electrical power to any sizeable region for more than 10 days would stop more than 70 per cent of all economic activity in that region. Given the costs involved to finance a traditional military attack, is it any surprise that cyber-warfare strategies are gaining attention?

CRITICAL DEFENCE

Perhaps the most unique aspect of cyber-warfare is its ability to be launched from anywhere in the world. Computers that are physically located in foreign countries may also be compromised and used as a launch platform for attack making identification of any initial attack source extremely difficult.

Cyber-attacks are inexpensive, easy to deliver and leave few fingerprints. Therefore, they will continue to remain a component of modern-day warfare. While countries around the world are in the process of integrating offensive and defensive cyber capabilities into their overall military strategies, the responsibility to protect high-value critical infrastructure targets will remain a significant challenge. Because of this, government and industry need to collaborate to develop protection strategies that carefully consider how a cyber war or attack could affect society and world economies.