America's Critical Infrastructure: Threats, Vulnerabilities and Solutions

Security managers must grasp the interface between physical and cyber threats

The tragic events of 9/11 awakened America to its critical infrastructure's vulnerabilities and to the threats to this infrastructure – both physical and cyber. In the almost two decades that passed since then, the ability to monitor, detect and defend against a wide slew of threats to critical infrastructure has increased considerably, as witnessed by the forests of video surveillance cameras and their attendant software and humanware controllers, surrounding almost every critical infrastructure site or facility. But, unfortunately, as the defenders became more sophisticated, so have the attackers and their capabilities.

A review of some of the evolving threats and vulnerabilities to America's critical infrastructure reveals a future no less dangerous than the situation today. The specter of stuck subway cars in deep underground tunnels, imperiling the lives of tens of thousands commuters, breached dams, threatening towns downstream, jammed telecommunications networks and megacities froze by electricity blackouts should – and do – cause many a security experts to lose sleep.

The Department of Homeland Security (DHS) defines critical infrastructures as assets that provide "the essential services that underpin American society and serve as the backbone of our nation's economy, security and health. We know it as the power we use in our homes, the water we drink, the transportation that moves us, the stores we shop in, and the communication systems we rely on to stay in touch with friends and family." Specifically, this includes 16 sectors: chemical, commercial facilities, communications, critical manufacturing, dams, defense industrial base, emergency services, energy, financial services, food and agriculture, government facilities, healthcare and public health, information technology, transportation, waste and wastewater, and nuclear reactors, utilities and waste.

With more than 80 percent of the critical infrastructure in the United States owned by the private sector, expensive security measures inevitably have to compete against an array of economic considerations, creating a reality where security alone is never the deciding factor. This creates two unique vulnerabilities:

- **Resource Disparity** - Cyber and physical security are an expensive venture, and require allocation of significant resources. While large companies and organizations can afford such outlays, small companies rarely can. This leaves essential critical infrastructure, such as many water utility outfits under-protected and exposed.
- **Outsourcing Complexity** - Today's companies and organizations tend to focus on core competencies and outsource all else to outside providers. This includes transportation, utilities, healthcare, financial service providers and many other companies. Quite often, physical and cyber protection services are also outsourced, making optimized defense

more complicated and creating more opportunities for leaked defense-related knowledge, procedures and data, and contributes to shortages of highly skilled personnel.

Critical Infrastructure Threats

Security and government officials are concerned about the vulnerabilities of America's critical infrastructure and the threats it faces now and in the foreseeable future. In a recent Reuters article, Dan Coats, Director of National Intelligence, said: "The system was blinking red. Here we are nearly two decades later and I'm here to say the warning lights are blinking red again," Coats specifically marked Russia, China, Iran and North Korea as "daily" attackers of America's computer networks, at federal, state and local government agencies level, in addition to U.S. corporations, and academic institutions.

There are three classes of threats to critical infrastructures:

- **Natural** - earthquakes, tsunamis, land shifting, volcanic eruptions, extreme weather (hurricanes, floods, draught), fires.
- **Human-Caused** - terrorism, rioting, product tampering, explosions and bombing, theft, financial crimes, economic espionage.
- **Accidental or Technical** - infrastructure and hazardous material failures and accidents, power-grid failures, water-treatment facilities failures, water-mains ruptures, safety-systems failures and a host of other disasters of omission and/or commission.

Cyber Threats

The list of cyber threats increases rapidly, as the number of hacking-sensitive platforms and potential victims increase, attracting more and more individual, private and state actors into the fray. The following list represents a partial set of typical threats (Source: GAO):

- Terrorists and other non-state actors seeking to destroy, incapacitate, or exploit critical infrastructures to threaten national security, cause mass casualties, weaken the economy, and damage public morale and confidence.
- Criminal groups, attacking systems, using spam, phishing, and spyware/malware, identity theft, online fraud, and computer extortion for monetary gain.
- Business intelligence operators, including criminal organizations, conducting voluntary and on-demand industrial espionage.
- Individuals and groups "grazing" the cyber world in search of victims, for a combination of thrill, monetary and "training" purposes.
- Bot-network operators, using networks, or botnets, of compromised, remotely controlled systems to coordinate attacks and to distribute phishing schemes, spam, and malware attacks.
- Disgruntled insiders, poorly trained employees, incompetent contractors – all creating the opportunities for outsiders to penetrate networks.
- National intelligence and psychological operations organizations, using cyber tools for information gathering, regime destabilization and as another arm furthering strategic goals.
- Spammers using the above methods to distribute unsolicited e-mail with hidden or false information to sell products, conduct phishing schemes, distribute spyware or malware, or attack organizations (e.g., a denial of service).

- National and/or commercial organization specializing in deploying spyware or malware against organizations or individuals, for political and commercial purposes.

Vulnerability by Concentration

One of America's more worrying critical infrastructure issues has to do with the fact that major portions of several critical sectors are concentrated in close geographic proximity; for example:

- **Energy** — 43 percent of America's oil refineries are located along the Texas and Louisiana coasts.
- **Chemical Industry and Hazardous Materials (chlorine)** — Over 38 percent of America's chlorine production is located in coastal Louisiana.
- **Transportation** — Over 33 percent of America's maritime container shipments pass through the ports of Los Angeles and Long Beach.
- **Transportation** — Over 37 percent of America's freight railcars pass through Illinois, and over 27 percent of America's freight railcars pass through Missouri.
- **Pharmaceuticals** — 25 percent of America's pharmaceuticals are manufactured in the San Juan Metropolitan Area, Puerto Rico.

Critical Infrastructure Protection - Market Size

According to the recent "Global Critical Infrastructure Protection Market 2018-2028", authored by ResearchAndMarkets.com, the North American critical infrastructure Protection (CIP) market is currently (2018) worth about $30 billion, and will be worth about $39 billion in 2028. Physical security, according to the report, is expected to account for the highest proportion of CIP spending, followed by network security. The largest segment in physical security expenditure will be the deployment of security-related personnel.

Vulnerable Critical Infrastructure Sectors

The following list explores some of the vulnerabilities identified in America's critical infrastructure:

Communications

The communications sector is huge and diverse, covering from traditional voice services, through all Internet-related services, to accessing all control devices in every other sector. Without properly functioning communications, it is difficult to imagine the smooth operation of business, public safety, transportation or government, to name but a few. Yet, the sector is vulnerable to extreme weather impact, as well as to the dangers of aging and terrorist attacks.

In July of 2001, for example, a freight train caught fire inside a Baltimore tunnel. The fire resulted in damage to several telecommunications and Internet backbone lines. This, in turn, led to several days of total or partial loss of communications and Internet service between Washington, D.C. and New England.

The 9/11 collapse of the World Trade Center towers resulted in flooding of one of the largest telecommunications nodes in the world. Millions of voice and data lines were disconnected,

leaving thousands of businesses (including the New York Stock Exchange) and residential customers without service for days.

With communications, an essential, integral part of every aspect of the U.S. economy, public safety and government, the economic and national security ramifications of a physical or cyber attack on even an isolated network are almost incalculable. These events come in conjunction with the increased vulnerability of this very same infrastructure due to inter-connectivity and growing complexity. With every signal light in every junction, every air-traffic control element interlinked though complex telecommunications networks, even an incidental interruption can easily mushroom into a colossal disruption of life and commerce. Of course, network designers and security experts are aware of these vulnerabilities and have developed mechanisms and procedures to contain and abate cyber and physical interferences with smooth operations, but the situation is far from secure.

America's cellular telephony network is one of the most vulnerable elements of the communications infrastructure. Cellular networks tend to collapse exactly when they're needed most – in the aftermath of a disaster.

Energy

The huge electricity blackout of 2003 in the Northeast demonstrated the fragility of America's aging and computer-dependent power grid. The aforementioned Northeast blackout cost around $5 billion in lost productivity and left nearly 50 million people in the dark. Indeed, disruption to the nation's energy supply (electricity and fuel) can mean an economic and security disaster of unimaginable scale.

The interdependence of America's power grid and the geographic concentration of America's refineries creates a vulnerability that certainly attracts the attention of terrorists; indeed, many experts think that energy systems are an attractive target to cyber-criminals/terrorists. But even the impact of an "innocent" natural disaster, such as a hurricane, can be unacceptable. The growing reliance of energy grids on system control and data acquisition (SCADA) systems, designed to automate processes such as power generation and distribution, coupled with the Internet-interfaces that service these systems, creates a vulnerability that is hard to belittle. Of course, the responsible authorities - in this case, the departments of Energy and Homeland Security - are aware of these vulnerabilities.

They established a National SCADA Testbed at the Idaho National Engineering and Environmental Laboratory to explore and mitigate against these very threats. It's important to remember that SCADA systems are not firewall-friendly, and can be slowed down considerably by intrusion detection and encryption activities. In fact, SCADA systems are so complex that many experts worry about self-inflicted failures, requiring no outside interference. Avoiding cascading failures of power grids, and overloaded redundancy systems require "brute" physical safety measures, such as inspections, no less than super-sophisticated counter cyber-threat activities.

Transportation

America's huge transportation network presents a complex and combined physical and cyber security challenge. While the almost total computerization of rail, air, and marine traffic invites

cyber terrorists' attention (and even just plain amateur hackers), the simplest physical disruption of rail or aviation hubs, due to human or nature-made events can rapidly mushroom into a damaging stoppage of essential human and commerce links. Add to this the fact that trains often carry large amounts of hazardous materials, sometimes in very close proximity to large concentrations of people and industry, and transportation networks are a prime axis of vulnerability, requiring constant attention and resources.

Maritime hubs present no less of a threat. Each and every shipping container is a potential guided missile and should be treated as such. A remote-controlled detonation of a container loaded with radiological waste products, such as those produced by almost every large-scale hospital around the world, can spread enough contamination and fear to freeze a huge seaport for months if not years, exacting an incalculable economic and psychological impact.

The security industry has responded to such threats with the development of complex human-machine systems designed to detect, alert and mitigate against maritime borne threats. Still, it's important to remember that terrorists have to detect only a single hole in the safety net, while defenders must maintain equally high vigilance along the entire front.

And of course, the aviation sector is also vulnerable and attractive to both physical and cyber threats, and as such has received and continues to receive enormous amounts of attention and resources from a wide spectrum of security-minded outfits – both private and governmental. Air cargo is a significant challenge that requires additional innovation; so far, the multi-layered approach adopted by aviation's security experts seem to provide a reasonable combination of deterrence, but red-team tests of security systems provide consistently discouraging results on the physical front, while cybersecurity presents a formidable challenge, if only because aviation's data and connectivity must be shared across a very wide array of users, such as airlines, traffic control hubs, and multiple security and intelligence centers – all terminating with people whose intentions and loyalty are almost always good but can prove damaging when/if they don't.

Government

The federal government has a dual role of ensuring the safety and security of the nation's critical infrastructure as well as of ensuring the safety and security of the government itself – another formidable critical building block in the critical infrastructure mosaic. DHS is the "quarterback" coordinating almost all of America's cyber and physical security efforts as they pertain to critical infrastructure. Indeed, the Department of Energy (DoE) is responsible for energy installations (including nuclear facilities); the Department of Treasury (DoT) is responsible for the safety and security of financial services infrastructure; the Environmental Protection Agency (EPA) is responsible for the nation's water infrastructure, and the Department of Health and Human Services (DHHS) is responsible for the nation's healthcare and human services infrastructure, and the Department of Agriculture (DoA), together with the DHHS is responsible for America's agriculture infrastructure.

The Federal Information Security Management Act (FISMA) is the driver of America's cybersecurity efforts. It is responsible for hardening networks against external attacks and internal misuse. Another body, National Cybersecurity Division (NCSD) constitutes the core of the DHS' cybersecurity effort to coordinate critical security information dissemination to federal agencies as well as to the private sector. Another governmental defensive tool is the Cyber

Warning and Information Network (CWIN), which links the DHS National Operation Center (NOC) to NOCs at other federal agencies and at telecommunications companies.

Evolving Threats

This section highlights a single, significant threat that is truly "over the horizon" but is shaping up as a major hurdle to the integrity of all critical infrastructure (and other) computer-based sectors.

Quantum computers and computing is becoming a reality, promising new achievements in computer science, data analysis, artificial intelligence, and machine learning. It also promises to create a new front of vulnerabilities in the very infrastructures it promises to better, principally by making existing encryption strategies and mechanisms much more vulnerable to penetration; without encryption, there will be no privacy and without privacy, there will be no security. Therein lays the future threat.

Specifically, the new, super-fast, computers will be able to break through the encryption of security certificates, enabling cybercriminals to perform sophisticated Man in the Middle (MITM) attacks, making Certificate Authorities and their service obsolete. One possible remedy to this upcoming vulnerability is to go the way of the Bitcoin and integrate decentralization into Public Key Infrastructures.

Another looming critical infrastructure threat worth mentioning is the constant presence of the threat of foreign interference with America's electoral infrastructure, and it's very democratic institutions; it is important to remember how vulnerable such systems are and what a huge effort is required to protect them.

Threats – both physical and cyber – against critical infrastructure in the United States and elsewhere are forecasted to increase over the coming years. It is the responsibility of government and private industry to remain ever cognizant of the responsibility they shoulder and therefore remain ever vigilant in their efforts to forestall current and upcoming threats. Security managers must learn to monitor simultaneously both physical and cyber threats understand the interface between them and constantly innovate for maximum resilience. The cost of failure is just too high.

About the author: *Johnathan Tal is the CEO of TAL Global, a leading Risk Management, Security Consulting and Investigative Agency serving clients all over the world. The San Francisco-based company is based in Silicon Valley with a large client base and a vast network of resources for the High-Tech, Hospitality, Manufacturing and Financial industries. Tal is also a Board Member at Qylur Intelligent Systems*