James A. Baker III Institute for Public Policy
Rice University

Hacks on Gas: Energy, Cybersecurity, and U.S. Defense

by

Christopher Bronk, Ph.D.

Fellow in Information Technology Policy
Director, Program on Energy and Cybersecurity, Center for Energy Studies
James A. Baker III Institute for Public Policy
Rice University

February 5, 2014

Abstract

Cybersecurity as it pertains to energy is a topic of increasing interest in both the U.S. government and private sector. Cyber incidents have impacted energy targets, as demonstrated by the Stuxnet and Shamoon cyber attacks. This paper, prepared for the U.S. Army War College's Strategic Studies Institute, considers cyber issues relevant to the Army and U.S. Department of Defense (DoD), including the electrical grid, oil and gas security, and the military's fuels supply chain. The DoD is incredibly reliant on private sources of energy, and the level of preparedness for cyber attack among those sources likely varies greatly. The author provides characterizations of these problems, as well as a set of policy prescriptions.

In the Beginning

Cybersecurity in the energy sector can trace its start to an account (that may or may not be true) about U.S. involvement in a computer-based attack on the energy infrastructure of the Soviet Union during the Cold War. Elements of the incident are described in the memoir of Thomas C. Reed, an official in the administration of President Ronald Reagan and a former National Reconnaissance Office director.

The incident, part of what is known as the "Farewell Dossier," involved KGB officer Vladimir Vetrov's service to French intelligence from 1981-82. Vetrov is alleged to have provided key Soviet technologies for both military and civilian applications, including computers used for process control in industrial technology. As the story goes, Vetrov's alleged counterintelligence work eventually led to the delivery of a faulty computer design to the Soviets. Designed to fail, the device allegedly caused a massive pipeline explosion in 1982, but there are differing accounts and disputes on the details. However, according to the CIA's Center for the Study of Intelligence, the U.S. supplied flawed technologies to the Soviet Union through the KGB's Line X intelligence effort:

> [The] CIA and the Defense Department, in partnership with the FBI, set up a program to do just what we had discussed: modified products were devised and "made available" to

> Line X collection channels. The CIA project leader and his associates studied the Farewell material, examined export license applications and other intelligence, and contrived to introduce altered products into KGB collection. American industry helped in the preparation of items to be "marketed" to Line X. Contrived computer chips found their way into Soviet military equipment, flawed turbines were installed on a gas pipeline, and defective plans disrupted the output of chemical plants and a tractor factory.[1]

Exactly what wound up where and produced what particular outcome is subject to debate. Jeffrey Carr, a security blogger and author, asserts that the Farewell cyber incident is no more than an "oft-repeated rumor" that has been generally accepted as fact. He asserts that the real cause was a pipeline operator ignoring warnings and allowing pressure to build, causing the catastrophic blast.[2]

While it's unclear if a major Siberian blast took place in 1982, operator error was likely to blame for an explosion in 1989, when natural gas liquids leaked adjacent to the Kuybyshev Railway near Ufa, Russia and passing trains ignited the resulting gas cloud. The major detonation killed more than 500 people.[3] In remarks to the Soviet Congress of People deputies, Mikhail Gorbachev attributed the explosion to pipeline operators miles away who, after noticing a drop in gas pressure, simply turned up the pumps rather than investigate the issue.[4]

Cyber Insecurity and Energy Security

Cybersecurity has grown to be a preeminent concern for the national security organs of the U.S.

---

[1] Gus Weiss, "The Farewell Dossier: Duping the Soviets," *Studies in Intelligence* 39, no. 5 (1996). Historical document posted online at the Center for the Study of Intelligence on April 14, 2007, https://www.cia.gov/library/center-for-the-study-of-intelligence/csi-publications/csi-studies/studies/96unclass/farewell.htm.

[2] Jeffrey Carr, "The Myth of the CIA and the Trans-Siberian Pipeline Explosion," *Digital Dao*, June 7, 2012, http://jeffreycarr.blogspot.com/2012/06/myth-of-cia-and-trans-siberian-pipeline.htm.

[3] Bill Keller, "500 on 2 Trains Reported Killed By Soviet Gas Pipeline Explosion," *New York Times*, June 5, 1989.

[4] Bill Keller, "Gas Blast and Uzbek Rioting Preoccupy Soviets," *New York Times*, June 6, 1989.

government.[5] Within certain circles, one need only say "cyber" to indicate the topic of cybersecurity. It has become an area of great interest, but in cybersecurity there is also tremendous ambiguity. How great is the threat to the United States? Its overseas interests? The U.S. economy or armed forces? Cybersecurity practitioners and experts have some idea, but there is a degree of hyperbole surrounding the issue and some heads in the sand as well.

How cybersecurity issues fit into energy puts some boundaries on the problems faced, but it is important to consider what is meant by "energy security." Writ large, energy security for the United States is the capacity for U.S. consumers—be they individuals, organizations, corporations, or government agencies—to gain access to the energy supplies they need or want.[6] Foreign embargos, tropical cyclonic activity, midstream plant disasters, and military action are all potential threats to energy security for the United States. Energy production in the U.S. is changing, however, and affecting how the U.S. meets its energy needs.

We cannot consider threats to energy security without acknowledging the rise of oil and gas production in the United States over the last decade. Computer-aided, horizontally drilled, hydraulically fractured oil and gas drilling has produced a dramatic rise in domestic production, now totaling some seven million barrels of oil per day[7] and 2.1 million cubic feet of natural gas per month.[8] U.S. production gains provide a degree of security from disruptions in international supply, but it is necessary to acknowledge that oil is traded on a global market, and regional gas markets may increasingly become interlinked over time. Thus a disruption in the Persian Gulf, East Asia, or Africa does not insulate prices paid for oil or even gas in the United States.

In addition to the supply of energy, including coal, nuclear power and other sources (each with its own environmental issues), there are the matters of processing and distribution. This represents the remainder of the energy supply chain, which among other items includes gas, coal,

---

[5] Executive Office of the President of the United States, "The Comprehensive National Cybersecurity Initiative," accessed January 27, 2014, http://www.whitehouse.gov/issues/foreign-policy/cybersecurity/national-initiative.
[6] For discussion on energy security as it applies to civil security, see Philip Cornell, "Energy Security as National Security: Defining Problems Ahead of Solutions," *Journal of Energy Security*, February 2009.
[7] Asjylyn Loder, "Fracking Pushes U.S. Oil Production to Highest in 20 Years," *Bloomberg*, January 9, 2013, http://www.bloomberg.com/news/2013-01-09/fracking-pushes-u-s-oil-production-to-highest-level-in-20-years.html.
[8] "U.S. Natural Gas Marketed Production," U.S. Energy Information Agency, October 31, 2013, http://www.eia.gov/dnav/ng/hist/n9050us2m.htm.

and nuclear power stations; electricity grids; oil and gas refineries; and pipelines. We should be concerned with cybersecurity in energy because, as with other areas of the global economy, computing has been widely adopted in the energy industry. Supercomputing is a key component to seismic analysis. Refineries are increasingly driven by Supervisory Control and Data Acquisition (SCADA) systems. The U.S. electrical grid has incorporated "smart" elements, including digital sensors, meters, and monitoring systems. The ubiquitous Internet Protocol interconnects many of these computers.

If there were no networked computers in the energy supply chain (from exploration to the pump or outlet), discussion of cybersecurity issues would be moot. But for decades, computation has been deeply incorporated into energy exploration, production, distribution, and consumption, as well as into the corporate and managerial activities supporting these activities. Thus, cybersecurity is an issue for the energy industry. While many scenarios posit a massive hack of the electricity system and its catastrophic failure, there are plenty of other more likely and less spectacular energy cybersecurity issues.

In prior Baker Institute research,[9] we identified three major cyber concerns in the oil and gas sector:

- Theft of core intellectual property;
- Disruption or destruction of a physical plant and other points of capital investment; and
- Compromise of communications by executive decision-makers regarding key business decisions.

Cybersecurity research related to energy is punctuated by breaches that align, to some degree, with the potential incidents we can imagine. It is important to remember that the Stuxnet worm (a piece of self-propagating malicious software) was ostensibly aimed at an energy target—the Iranian nuclear enrichment infrastructure. Another worm, Shamoon, spread rapidly across the personal computers of Saudi Aramco at an incredible speed, deleting the contents of perhaps as

[9] Chris Bronk and Adam Pridgen, "Policy Report 53 – Cybersecurity Issues and Policy Options for the U.S. Energy Industry," James A. Baker Institute III for Public Policy, Rice University, September 2013, http://bakerinstitute.org/research/baker-institute-policy-report-53-cybersecurity-issues-and-policy-options-for-the-us-energy-industry/.

many as 30,000 hard drives and also impacting systems at other companies.[10]

What such cyber attacks mean to U.S. energy security and the security of energy needed by the U.S. Department of Defense (DoD) requires some consideration. At a global level, we need to consider how likely an oil or gas disaster produced or facilitated by cyber means actually is and what can be done to mitigate that threat. For the DoD, important questions need to be raised about the security of computer systems employed in the distribution of electricity and fuels from major bases to forward deployed elements in contact with hostile forces.

There are likely three major areas of energy-related cyber vulnerability that are relevant to the U.S. Army: (1) the provision of electricity to bases and facilities by the electrical grid, both in the United States and abroad; (2) the distribution of fuels to forces often operating some distance from major logistical hubs; and (3) major cyber attacks against suppliers of fuels that would result in a significant disruption of supply or a rise in price. Other scenarios of attack are no doubt possible and are limited only by vulnerability, technical know-how and imagination. This is very much a ranked order, however, as cyber attacks against the grid are alarming and potentially achievable. Cyber attacks against Army logistics should be taken as a given, and a massive cyber attack against the oil and gas industry would be of great concern far beyond the DoD.

Cyber Attack Against the Electricity System

In a 2008 report, the Defense Science Board stated that "critical national security and Homeland defense missions are at an unacceptably high risk of extended outage from failure of the grid." In 2006, the DoD consumed some 3.8 billion kWh of electricity and spent $3.5 billion for energy to fixed installations. Electricity services for the DoD are sourced overwhelmingly from the private sector. "About 85% of the energy infrastructure upon which DoD depends is commercially owned, and 99% of the electrical energy DoD installations consume originates outside the fence." The electricity grid is characterized by the DSB as "fragile, vulnerable, near its capacity

[10] Chris Bronk and Eneken Tikk-Ringas, "The Cyber Attack on Saudi Aramco," *Survival: Global Politics and Strategy* 55, no. 2 (2013).

limit, and outside of DoD control."[11]

Threats to the stable operation of the grid include overload, natural phenomena such as earthquakes or storms, physical acts of sabotage, and cyber attack. The broad impact of major outages and a prolonged disruption of the electrical grid have been felt by many in the United States. A blackout in the northeast on August 14, 2003, affected as many as 50 million Americans and Canadians. Hurricane Sandy, which struck the New York City metropolitan area late in autumn at Category 3 force, left as many as 7.9 million customers without power, many for a week or more.

Before delving into hypothetical cyber attacks on the electrical grid, it is important to note how an electrical grid can fail, as well as the problems faced in restoring electrical service. In the 2003 blackout, the cause was improper trimming of trees near a power line, which led to a series of cascading failures. It is necessary to emphasize the relevance of these cascading failures, and the amplified butterfly effect of one small disruption potentially triggering a major fault in the system. When the grid overloads, electricity production is taken offline until the load can be successfully rebalanced. The restoration process may be hampered by damage to key components for which spare inventories are generally scarce and producers few.[12]

This system—one that is highly dynamic, but needing to remain in equilibrium between supply and demand; prone to cascading failures; and posing significant difficulty in repair—is why there is great concern in policy and cybersecurity circles regarding its vulnerability to cyber attack. The grid is also changing rather rapidly. Among the most visible manifestations of this change were utility company deployments of smart grid technologies funded with $11 billion under the American Recovery and Reinvestment Act of 2009 and by private investments.[13]

---

[11] Defense Science Board, *Report of the Defense Science Board Task Force on DoD Energy Strategy* (Washington, DC: US Department of Defense, May 2008), 18.
[12] Gal Luft, "Ten years after the Northeast Blackout: How secure is our grid?" *Journal of Energy Security*, August 2013.
[13] US Department of Energy, "Recovery Act: Smart Grid Investment Grants," accessed January 27, 2014, http://energy.gov/oe/technology-development/smart-grid/recovery-act-smart-grid-investment-grants.

Smart grid technologies are intended to bring computational resources to the management of the electrical grid. While the most common and visible pieces of the smart grid systems being deployed in the United States are digital meters appearing where spinning dial analog meters once resided, smart grid activities are designed to do much more than change the measurement vehicle for billing. A smart grid implementation should offer enhanced reliability, increased efficiency, and load adjustment, as well as the capacity to incentivize use of electricity outside of peak use periods. An additional argument for a smart grid, falling under the category of "reliability," is the potential to better observe damage to the physical infrastructure through the deployment of sensors throughout.

It is this deployment of computer-driven sensors and other devices designed to change the state of the electrical grid that is of concern with regard to cybersecurity. Deployment of Supervisory Control and Data Acquisition (SCADA) systems in electricity is an ongoing activity, as it is in all manner of other sectors, from manufacturing to water distribution. What is relatively new is the networking of these SCADA devices together. Deployment of SCADA devices and other pieces of computing hardware into the electrical grid expands its notional attack surface.[14]

How much this attack surface is exposed to unauthorized users and vulnerable to manipulation is the key question. Setting aside the worst case, such as scenarios of a massive disruption bringing down the grid for weeks or months, there are many unanswered questions about how we can measure the degree to which deployment of computing throughout the grid has made its ongoing operation riskier. But we know from attempted and successful physical attacks on the grid that there are vulnerabilities.

In April 2013, an assailant or assailants fired more than 100 rifle rounds into a Pacific Gas and Electric substation in San Jose, California, severing nearby fiber optic cables in the process.[15] The FBI is investigating the matter. On August 21, 2013, power transmission lines were severed in Central Arkansas. Two days later, a fire was set at an Extra High Voltage switching facility

---

[14] Kim Zetter, "Researchers Uncover Holes That Open Power Stations to Hacking," *Wired*, October 16, 2013, http://www.wired.com/threatlevel/2013/10/ics/.

[15] "Vandalism at San Jose PG&E Substation called 'sabotage,'" *CBS*, April 16, 2013, http://sanfrancisco.cbslocal.com/2013/04/16/gunshots-cause-oil-spill-at-san-jose-pge-substation/.

nearby.[16] The alleged assailant in the Arkansas cases was apprehended and indicted, and disruption in both incidents was fairly minimal.

A widely confirmed, well-documented cyber attack against the electrical grid that definitively demonstrated a disruption of service has not occurred. Rumors abound, but reliable evidence is scant. The Idaho National Lab did stage a cyber attack on a generator, causing it to self-destruct in 2007. On the matter, known as Aurora, security technologist Bruce Schneier commented:

> I haven't written much about SCADA security, except to say that I think the risk is overblown today but is getting more serious all the time—and we need to deal with the security before it's too late. I didn't know quite what to make of the Idaho National Laboratory video; it seemed like hype, but I couldn't find any details.[17]

Several years later, such an attack remains largely hypothetical, although the Stuxnet cyber attack against the Iranian nuclear program's enrichment facilities demonstrated the viability of a cyber attack against a SCADA system in an energy facility. In the wake of Stuxnet, the North American Electric Reliability Corporation (NERC) published a major cyber attack task force review providing guidance to the electricity sector beyond the cyber elements of its NERC–Critical Infrastructure Protection (NERC-CIP) standards.[18]

Beyond NERC, Congress has taken up the issue of electricity vulnerability to cyber attacks. In 2013, Edward Markey, then a U.S. Representative from Massachusetts, and Rep. Harvey Waxman released a report based on surveys sent to over 150 utilities and other providers of electricity in the United States. The report concluded that utilities are regular cyber attack targets, and that while they comply with mandatory standards, they often do not implement voluntary NERC recommendations. What remains unclear is how often the electrical sector is attacked in a

---

[16] "Federal Grand Jury Returns 8-count indictment Against Jason Woodring," U.S. Attorney's Office, Little Rock, Arkansas, November 6, 2013, accessed January 15, 2014, http://www.fbi.gov/littlerock/press-releases/2013/federal-grand-jury-returns-eight-count-indictment-against-jason-woodring.

[17] Bruce Schneier, "Staged Attacks Causes Generator to Self-Destruct," *Schneier on Security*, October 2, 2007, https://www.schneier.com/blog/archives/2007/10/staged_attack_c.html.

[18] North American Electric Reliability Corporation, "Cyber Attack Task Force Final Report," May 9, 2012. See also NERC and NERC-CIP guidance at "CIP Standards," North American Electric Reliability Corporation, http://www.nerc.com/pa/Stand/Pages/CIPStandards.aspx.

manner that directly targets SCADA systems impacting production or distribution of electricity. While actors in the electricity sector may be "attacked," the definition of a cyber attack is broad, so that anything from viruses to email phishing campaigns is counted as an attack. However, the security of relevance to national security is an attack against the computing infrastructure directly involved in getting power to customers.

While discussion on electricity and cybersecurity is largely focused upon disruption via compromise of SCADA systems, Xie, Mo, and Sinpoli[19] build upon an intriguing scenario of a false data injection attack against state estimates in deregulated electricity markets posited by Liu, Reiter, and Ning.[20] They contend that energy demand reported from the grid by computerized sensors could be replaced with false information. Such activity could then be used to subvert the function of the pricing market for electricity. While both papers represent a hypothetical vulnerability, informal reporting from electricity distributors indicates that, if anything, deployment of smart grid sensing facilitates rapid detection of electricity theft. We can assume that where such theft occurred by cyber means without swift remedy, it might go undetected for some time.

Clearly, cybersecurity and electricity in the United States and abroad present many issues of concern. The DoD would be well served to carefully engage in efforts similar to those undertaken by the Department of Homeland Security to improve the cyber defenses of industrial control systems deployed in electricity.[21] How exactly the DoD would do this in an atmosphere charged by the Snowden leaks and valid industry concerns of onerous and imprecise federal regulations on cybersecurity is to be determined. Nonetheless, there is a real threat, and the most significant issues likely remain either unknown or unreported. This is likely also the case in oil and gas production as well.

---

[19] Le Xie, Yilin Mo, and Bruno Sinopoli, "False Data Injection Attacks in Electricity Markets," presentation at the First IEEE International Conference on Smart Grid Communications, Gaithersburg, Maryland, October 4–6, 2010.
[20] Yao Liu, Peter Ning, and Michael Reiter, "False Data Injection Attacks against State Estimation in Electric Power Grids," *ACM Transactions on Information and System Security* 14, no. 1 (May 2011).
[21] See mention of the DHS industrial control system security efforts below.

Hacking the Oil and Gas Sector and the DoD Energy Supply Chain

Cyber threats to energy production in the oil and gas sector are of rising concern to industry and government. Like participants in other major industries, oil and gas firms are frequently targets of espionage activity, which has heavily migrated online. But a less generic concern is the targeting of critical infrastructure employed to produce, transport, refine, and distribute oil and gas. This issue was summarized in a 2013 report by the Council on Foreign Relations:

> [A] major risk facing the oil and gas industry is the disruption of critical business or physical operations by attacks on networks. As information technology's role in all phases of oil and gas production—from exploration and production to processing and delivery—expands, the vulnerability of industry operations to cyberattacks increases. A hacker with the right tools, access, and knowledge could, for instance, identify the Supervisory Control and Data Acquisition systems (SCADA) and industrial control systems (ICS) used to operate critical infrastructure and facilities in the oil and gas industry and that are connected to the Internet.[22]

Much like electricity, there is reason for significant concern about cyber attacks against the infrastructure of the oil and gas industry. SCADA systems abound in production and refining operations, and there is valid concern that a compromise of such a system could produce a major spill or explosion. Security of SCADA computing is the primary mission of the U.S. Department of Homeland Security's Industrial Control System–Cyber Emergency Response Team (ICS-CERT). ICS-CERT's core mission is to provide the operators of SCADA systems with warnings of threats or compromises that would damage business operations or the public at large.

The Shamoon malware incident of August 2012 was perhaps the most significant cyber attack to be directed against the oil and gas industry. Delivered to the computer network of Saudi Aramco, likely by insertion upon a computer inside a company facility, Shamoon significantly impacted the computer network and computing infrastructure of the company. According to Aramco

[22] Blake Clayton and Adam Segal, *Addressing Cyber Threats to Oil and Gas Suppliers*, Council on Foreign Relations, June 2013.

officials, it did not impact production by the Saudi national oil company. What Shamoon did do was delete the digital contents of computer hard drives, very quickly.[23] Perhaps as many as 30,000 computers were affected at Aramco,[24] plus additional machines at RasGas, a joint venture of QatarGas and Exxon-Mobil. Because Shamoon was a piece of self-propagating software, concern over its spread leapt beyond Aramco, which was the ostensible target, to companies providing services to Aramco, and quite possibly to almost any organization interfacing with the Aramco network.

According to Aramco, Shamoon did not impact oil and gas production, indicating that it did not jump to computers involved in that production. Fear of a cyber attack able to impact computers responsible for driving physical infrastructure is a foremost concern in the oil and gas sector, both as a security and safety issue. A related concern is the compromise of process control computing in the petrochemical industry. While we are accustomed to hearing of Cyber Pearl Harbor scenarios, there is the potential for considerable loss of life or environmental damage from a "Cyber Bhopal" event.

Ralph Langer, who contributed heavily to the reverse engineering of the Stuxnet malware, made important points on this oft-neglected area for concern. In an interview with former NSA general counsel and DHS official Stewart Baker, he stated,

> Chemical plants run on industrial control systems; they could be remotely instructed to release gases that will kill the people in surrounding neighborhoods in a Cyber Bhopal scenario. That's a huge problem because there are several thousand potential chemical targets in the U.S. alone.[25]

---

[23] John Roberts, "Cyber threats to energy security, as experienced by Saudi Arabia," *Platts*, November 27, 2012, http://blogs.platts.com/2012/11/27/virus_threats/.
[24] Elinor Mills, "Saudi Oil firm says 30,000 computers hit by virus," *CNET*, August 27, 2013, http://news.cnet.com/8301-1009_3-57501066-83/saudi-oil-firm-says-30000-computers-hit-by-virus/.
[25] Stewart Baker, "Cyberwar and Industrial Controls: A Conversation with Ralph Langner," *The Volokh Conspiracy*, November 18, 2012, http://www.volokh.com/2012/11/18/cyberwar-and-industrial-controls-a-conversation-with-ralph-langner/.

While the possibility of subverting the systems of the petrochemical industry remains a hypothetical scenario, the response to such an event would most certainly require intervention of federal agencies. This is an obvious homeland security concern and one that will require diligence from the petrochemical industry as well as the intelligence community. Broader concern about a massive hack disabling the oil and gas sector should be bounded by an understanding of what can be attacked and how.

The probability of a massive cyber attack disabling the oil and gas industry's production, refining, and distribution likely is very low, as each piece of infrastructure is generally constructed with computing components available at the time of construction, possesses a far more limited feature set, and is usually designed to perform a single function. An attack like Shamoon was able to be significant because it compromised a massive number of homogenous computer systems designed to run a fairly broad set of applications. Achieving the same impact against a massive number of Programmable Logic Controllers (PLCs) across multiple facilities is a far more difficult task to accomplish.

For the DoD, vulnerability exists in the distribution of fuels, where there are also likely issues of cyber attack and disruption. Much like other large organizations, the DoD has adopted networked computers for all manner of administrative and logistical activity. The Defense Logistics Agency (DLA) holds the mandate for fuels provision for the armed services and has developed enterprise computing tools to perform its fuels supply mission.

Since the 1990s, the DoD has built upon the Fuels Automated System (FAS) a variety of applications that now fall under the label of the Enterprise Business System (EBS).[26] DoD fuels management is paperless, and utilizes Windows-based client-server applications and Web-based applications where data is entered and received via an Internet browser. Rather than develop an entirely bespoke fuels management system, DLA has deployed an Enterprise Resource Planning (ERP) software package including commercial, off-the-shelf (COTS) technology, including

[26] United States Office of the Director, Operational Test and Evaluation, "DoD Programs: Fuel Automated System (FAS)," FY 2002 Annual Report, http://www.dote.osd.mil/pub/reports/FY2002/pdf/dod/2002FAS.pdf.

components from SAP, the self-described market leader in enterprise application software.[27] Employment of commercial software allows it to be run on commodity computer hardware, such as Intel-based personal computers and servers running the Windows operating system. This has been done for economic reasons, as the Windows-Intel platform has grown to near ubiquity in the U.S. government and throughout corporations in the United States. DLA's EBS Energy

Convergence program will deploy further SAP elements designed to function easily with oil and gas industry standards and practices.[28]

Regarding cybersecurity of fuels data, a sophisticated attacker is likely aware that DoD is running SAP products on the DoD's Non-classified Internet Protocol Router Network (NIPRNet), which includes connectivity to the public Internet. While other DoD networks are protected by an air gap, a complete physical disconnect from networks connected to the Internet, the logistical activities of the DoD are primarily unclassified and Internet-connected so as to benefit from automation in business processes accepted as proper practice in logistical activities. This is not aberrant behavior, as maintaining a classified computing environment to manage fuel acquisition and distribution with private sector organizations would be technically infeasible and uneconomical.

The question then turns to how secure the systems employed in managing fuels for the DoD may be. Evidence of the level of cybersecurity on DoD fuels systems is fairly scant, with the exception being a 2006 DoD Office of Inspector General audit on information security controls in the DLA's business systems modernization. It noted a number of IT security problems in the EBS modernization, including: incomplete system certification and accreditation; failures in addressing security weaknesses; incomplete user management procedures; inconsistency of security training; and out-of-date continuity of operation plans.[29]

---

[27] Defense Logistics Agency, "Enterprise Business System (EBS)," accessed January 28, 2014, http://www.dla.mil/informationoperations/pages/EBS.aspx.
[28] Michael Broderick, "Energy Business System Energy Convergence," PETRO Conference, May 2012.
[29] United States Inspector General, "Information Technology Management: Review of the Information Security Operational Controls of the Defense Logistics Agency's Business Systems Modernization Energy," D-2006 -079, Department of Defense, April 24, 2006, http://www.dodig.mil/Audit/reports/FY06/06-079.pdf.

The EBS audit results, however, do not necessarily reflect upon the capacity of DLA's software to stand up to a cyber attack; rather, they highlight organizational shortcomings in meeting cybersecurity requirements spelled out in the provisions of the 2002 Federal Information Security Management Act (FISMA). In 2006, the Office of Management and Budget gave the DoD a failing grade for its FISMA report. But OMB's measurement of cybersecurity efforts, and indeed any relation between FISMA scores and maintenance of an effective cybersecurity effort at an agency level, has been questioned. Richard Bejtlich, a well-regarded cybersecurity expert, expressed his opinion of the process when the 2006 scores were released. He argued, "Agencies with high scores are no more secure than agencies with low scores. High-scoring agencies just write good reports, because FISMA is a giant paperwork exercise that makes no difference on the security playing field."[30]

That DLA has difficulty meeting all of the requirements of FISMA in deploying computer systems should be no surprise. What is important, however, is the capacity for resilience, which ensures continuity of operations for DoD and Army fuels logistics. This appears to be a rising trend in cybersecurity, as the mindset shifts from a network defense model in which the goal is to keep intruders out, to one where resiliency and recovery are embraced as core objectives.

Cyber and Energy: Some Prescriptions

Some time ago a colleague asked a well-regarded cybersecurity analyst for some guidance on a message for top corporate leaders regarding the problems faced by their IT security staff. He offered the following. "The Chinese are on your network and you probably know about it; the Russians are on it and you probably don't know about it; and give up." While the U.S. Army clearly can't give up on cybersecurity, an acceptance of cyber vulnerability is required with regard to its computer systems and those upon which it depends to perform its missions.

In coping with cyber security issues as they pertain to energy security matters, it is worthwhile to consider several items moving forward.

---

[30] Richard Bejtlich, "FISMA 2006 Scores," *Tao Security*, April 12, 2007, http://taosecurity.blogspot.com/2007/04/fisma-2006-scores.html.

1. Recognize that cyber incidents like safety or disruption events are not just organizational issues, but also issues of potential concern across an extensive, interconnected energy supply chain.
2. Develop trusted third party and clearinghouse relationships aimed at developing better cyber intelligence and analysis.
3. Produce and constantly refine models of cyber risk intelligence, merging the valuation of assets/processes, threats, and reasons for potential compromise.
4. Consider the cybersecurity ramifications as the Internet expands to cover more and more infrastructure, including hundreds of millions of energy-related computing devices.
5. Connect the spheres of geopolitics and the technical aspects of cybersecurity to develop holistic models for coping with the cybersecurity problem.

These recommendations represent an initial thrust of activity, but instituting them will require difficult shifts in behavior for government and industry. Additionally, it is worth considering how cyber incidents can play out very quickly. For instance, the compromise of the Associated Press's Twitter feed by the Syrian Electronic Army and its transmission of a bogus tweet regarding an attack on the White House led to the issuance of a high volume of sell orders in the New York Stock Exchange due to trading algorithms that "read" the tweet. In less than two minutes, the value of the NYSE fell by roughly $136 billion. The index recovered quickly, but there were both winners and losers on the deal. Although the energy industry may not hold a similar sort of vulnerability, we must assume that foreign adversaries, including states and transnational actors, will target it. Deep analysis not only on vulnerability, but also on the resiliency of the energy supply chain to cyber attack is therefore necessary.