COUNCIL on
FOREIGN
RELATIONS

ENERGY BRIEF

Addressing Cyber Threats to Oil and Gas Suppliers

Blake Clayton and Adam Segal

June 2013

This brief is made possible through the generous support of the Alfred P. Sloan Foundation.

The Council on Foreign Relations (CFR) is an independent, nonpartisan membership organization, think tank, and publisher dedicated to being a resource for its members, government officials, business executives, journalists, educators and students, civic and religious leaders, and other interested citizens in order to help them better understand the world and the foreign policy choices facing the United States and other countries. Founded in 1921, CFR carries out its mission by maintaining a diverse membership, with special programs to promote interest and develop expertise in the next generation of foreign policy leaders; convening meetings at its headquarters in New York and in Washington, DC, and other cities where senior government officials, members of Congress, global leaders, and prominent thinkers come together with CFR members to discuss and debate major international issues; supporting a Studies Program that fosters independent research, enabling CFR scholars to produce articles, reports, and books and hold roundtables that analyze foreign policy issues and make concrete policy recommendations; publishing *Foreign Affairs*, the preeminent journal on international affairs and U.S. foreign policy; sponsoring Independent Task Forces that produce reports with both findings and policy prescriptions on the most important foreign policy topics; and providing up-to-date information and analysis about world events and American foreign policy on its website, CFR.org.

The Council on Foreign Relations takes no institutional positions on policy issues and has no affiliation with the U.S. government. All views expressed in its publications and on its website are the sole responsibility of the author or authors.

For further information about CFR or this paper, please write to the Council on Foreign Relations, 58 East 68th Street, New York, NY 10065, or call Communications at 212.434.9888. Visit CFR's website, www.cfr.org.

INTRODUCTION

Cyber threats to oil and gas suppliers pose an increasingly challenging problem for U.S. national security and economic competitiveness. Attacks can take many forms, ranging from cyber espionage by foreign intelligence services to attempts to interrupt a company's physical operations. These threats have grown more sophisticated over time, making them more difficult to detect and defend against. So, too, have the actors behind them, which have evolved from lone hackers with few resources to state-sponsored teams of programming experts. Several of the world's major oil and gas producers, including Saudi Aramco (officially the Saudi Arabian Oil Company) and Qatar's RasGas, have fallen victim to cyberattacks since 2009. Others, such as Chevron, have also had their networks infected.[1]

Some damage was done in each of these cases, but the costs of future breaches could be much higher, whether to corporate assets, public infrastructure and safety, or the broader economy through energy prices. Successful cyberattacks threaten the competitiveness of the U.S. oil and gas industry, one of the nation's most technically advanced and economically important sectors.

While intrusions previously focused on the theft of intellectual property and business strategies, the malware attack on Saudi Aramco reflects a worrying qualitative change toward attacks with the potential for causing physical disruptions to the oil and gas supply chain.

THE NATURE OF OIL AND GAS CYBER THREATS

The actors behind cyberattacks on the oil and gas industry vary, as do their objectives and methods. Foreign intelligence and defense agencies, organized criminals and other nonstate groups (some of which do state-sponsored work), and freelance hackers have all been linked to infiltrations against private-sector targets, including energy firms.[2] So have insiders—those with privileged access to a company's computer network—such as former or current employees or contractors. The methods that attackers use against oil and gas companies are evolving, as are methods used against the private sector more broadly.

Cyber threats to oil and gas production can be grouped into two categories. The first is cyber espionage, which consists of third-party attempts to covertly capture a company's sensitive internal communications or data with the goal of gathering national security or commercial intelligence.[3] Over the last several years, oil and gas companies have become more vulnerable to this type of exploitation as their operations have become more reliant on digitally transmitted information. The disclosure of proprietary information can undercut a company vis-à-vis its peer firms, and even jeopardize its survival over time. American oil and gas firms are subject to frequent and often successful attempts by insiders, competitors, and foreign governments to access their trade secrets, such as long-term strategic plans, bids tendered for new drilling acreage, and private negotiations with foreign officials. Hackers have been successful in stealing oil companies' handbooks and geologic data, according to industry reports. Many other companies have likely fallen victim to these tactics without ever realizing it, though it is impossible to know for certain how widespread never-uncovered attacks are.[4]

Arguably the most successful known campaign against American oil and gas firms is one dubbed "Night Dragon" by McAfee, the cybersecurity firm that first disclosed its existence. According to McAfee, Night Dragon was a "coordinated, covert, and targeted" campaign by China-based hackers to obtain confidential data from five major Western energy companies, beginning around 2008 and extending into early 2011. Night Dragon was able to steal gigabytes of highly sensitive material, including proprietary information about oil- and gas-field operations, financial transactions, and bidding data.[5] It is difficult to tell if and how any of this information was used. One U.S. oil executive interviewed said he believed that on at least one occasion a rival national oil company appeared to know his firm's bidding plans in advance of a lease auction, which resulted in his losing the bid.[6] Security experts believe Night Dragon is only one of several similar attacks, of which oil and gas companies are either unaware or afraid to disclose publicly for fear of displeasing investors.[7]

The second 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.[8] Once in the system, an infiltrator could in theory cause the flow of natural gas through a pipeline to grind to a halt, trigger an explosion at a petrochemical facility, or do damage to an offshore drilling rig that could lead to an oil spill. Such threats now have the potential to cause environmental damage, energy-supply outages for weeks or months, and even the loss of human life.

Though there are no known cases of an attack on an oil- or gas-related target damaging physical operations, U.S. security experts believe this risk is increasingly real.[9] In February 2013, for example, malware unintentionally downloaded by workers incapacitated networks on some rigs and platforms.[10] Two months later, U.S. officials revealed that a wave of attacks on U.S. corporations, particularly energy companies, had been underway for several months. The attacks, which were unsuccessful in compromising their intended targets, appeared to have originated in Iran. Their objective was apparently to destroy data and take control of critical ICS. One official described these attempts as "probes that suggest that someone is looking at how to take control of these systems."[11]

Two incidents, the use of Stuxnet against Iran's nuclear enrichment facilities in 2009 and of Shamoon on Saudi Aramco's computer network in 2012, illustrate this growing threat.[12] Stuxnet, a virus widely believed to have been developed by the United States and Israel, altered the code that drives programmable logic controllers (PLCs), the computers that control automated industrial processes, while hiding the changes from the target's operators.[13] By distorting the Siemens software used by the centrifuges to enrich uranium at the Natanz nuclear facility, as the virus was apparently designed to do, Stuxnet demonstrated the ability of malware to at least partially derail critical industry machinery.[14] A similar approach might be used to target oil and gas infrastructure in the future.

In a second cyberattack, which occurred in August 2012, the so-called Shamoon malware struck Saudi Aramco, Riyadh's state oil giant, destroying data on—and ultimately disabling—approximately thirty thousand computers. The attack was likely perpetrated by someone with inside access to the company's network and delivered using a small USB drive.[15] Though the code itself was relatively unsophisticated, former secretary of defense Leon Panetta called the incident "probably the most destructive . . . that the private sector has seen to date."[16] Aramco's oil production was apparently unaffected by the episode, though some security experts believe the attack could have been damaging had it penetrated further into the network.[17] The attack still harmed the company's productivity, however, by rendering tens of thousands of computers useless.

A cyberattack capable of obstructing an energy company's physical operations is more difficult to pull off than the typical data heist. In the 2012 Aramco attack, for example, a thumb drive loaded with relatively unsophisticated malware ran on the company's network, apparently causing millions of dollars of damage.[18] Though the attack seemingly aimed to disrupt oil production, it was purportedly unable to interrupt Aramco's physical operations. Penetrating deeply enough into a major energy company's network to interfere with its ICS typically requires familiarity with the structure of the network, a way of accessing the network from the inside, and sophisticated code designed to exploit the targeted system. To meet these operational hurdles would typically require significant planning, financial resources, technical expertise, and inroads within the corporation or facility being targeted. Though high, these barriers would not be insurmountable to certain skilled operators, many of whom work for or under the auspices of foreign governments or are available to them for hire.

Stuxnet and Shamoon also demonstrate how cyberattacks may spread beyond their initial targets and inflict damage on oil and gas companies. Not long after Stuxnet appeared in Iran, it infected Chevron's computer systems, though it left no damage. RasGas (a joint venture between Qatar and ExxonMobil) was not as fortunate. Two weeks after Shamoon struck Saudi Aramco, the same virus hit the giant Qatari natural-gas firm and disabled its website and email servers. Both incidents might have been the result of this malware migrating beyond its intended targets rather than deliberate attacks on either Chevron or RasGas, judging by the close ties between oil and gas companies operating in the Middle East and the similarities in the source code.[19]

THE STAKES

The probability of and damages likely to result from different kinds of cyberattacks against oil and gas targets vary enormously. Successful acts of cyber espionage against the sector are ubiquitous and ongoing. General Keith Alexander, director of the National Security Agency (NSA) and head of the U.S. Cyber Command, estimated in 2012 that cyber crime costs U.S. businesses $114 billion a year, with another $250 billion lost in stolen intellectual property.[20] The energy sector, including oil and gas producers and infrastructure operators, was hit by more targeted malware attacks over a six-month period in 2012 than any other industry, according to one study.[21] Energy companies were targeted in 41 percent of the malicious software–attack cases reported to the Department of Homeland Security (DHS) ICS team in 2012.[22] The costs to any particular firm are highly specific, depending in part on the robustness of the firm's security posture and its attractiveness as a target.

In almost all cases of cyber espionage, the losses accrue as a steady drip of lost profit via unfairly empowered competitors and resources diverted to cybersecurity-related expenses rather than through one sudden catastrophic blow. But the harm that such attacks can do to the United States when U.S. firms are targeted is real.

In contrast, cyberattacks on oil and gas companies with physical consequences will likely remain rare, though the damages due to successful attacks could be sizeable. Attacks are more likely to pose a public-relations problem (by altering a company's website, for instance) or disrupt business operations (such as email servers) than upset critical physical infrastructure, which is typically harder to penetrate. But the SCADA systems that undergird the modern oil and gas supply chain are not invulnerable.[23] The relatively recent evolution of SCADA systems from a "single, centralized supervisory system to a decentralized series of interconnected networks" has made them easier to compromise, in some cases, than less sensitive information technology.[24] If infiltrated, they could cause assets like pumping stations or catalytic crackers to shut down or, worse, malfunction and destruct. The immediate damage from an attack that physically disrupts oil and gas production could include local environmental harm, commercial losses, and on-site workforce casualties.

WAYS FORWARD

The U.S. government is trying to address cyber threats by improving security at home and engaging friends and potential adversaries abroad. DHS has asked its Industrial Control Systems Cyber Emergency Response Team (ICS-CERT) to help in the defense of control systems, including in the oil and gas sector, through response and the timely sharing of threat information. In 2011, the Department of Energy (DOE) launched the Cybersecurity for Energy Delivery Systems program "to assist energy sector asset owners" in power, oil, and natural gas by partnering with industry to "develop cybersecurity solutions for energy delivery systems through integrated planning and a focused research and development effort."[25]

In February 2013, President Barack Obama signed an executive order to improve cybersecurity for critical infrastructure.[26] That order instructs DHS, the Department of Justice, and the director of national intelligence to share more information with operators of privately owned critical national infrastructure, including oil and gas producers. The order also expands the Enhanced Cybersecurity Services, a program that shares cybersecurity threat information with defense contractors, to critical infrastructure companies. In an effort to raise security standards in the private sector but not overregulate, the order also calls for the establishment of a "cybersecurity framework." This is a voluntary set of cybersecurity best practices, developed by the National Institute of Standards and Technology in conjunction with oil and gas producers. DHS has been instructed to work with DOE and other agencies, as well as industry councils, to implement the best practices laid out in the framework and identify incentives for companies to join the voluntary program, though incentives that might be attractive to oil and gas producers such as tax breaks or liability protections must come through legislative action.

Industry executives appear skeptical, however, about whether these various efforts will be enough, expressing concern in particular about delays in sharing information between government sources and industry participants who need it. These doubts have been exacerbated as several pieces of broad cybersecurity legislation that would apply to U.S. oil and gas producers have been derailed by arguments over how best to share threat information between the government and the private sector, among other issues.[27] Yet information sharing should be the central focus of U.S. efforts to improve cybersecurity for oil and gas. Providing more effective mechanisms for sharing threat information among firms and between the public and private sectors might make it more difficult for hackers to exploit an industry-wide vulnerability to move from one target to another. The Obama administration should reevaluate the classification level of threat information to make it easier to share with the oil and gas industries. Indeed, there are concerns within the intelligence community that classification is too strict. For example, General Michael Hayden—former director of the NSA and Central Intelligence Agency—repeatedly said that information regarding threats is overclassified.[28]

The February 2013 executive order may improve information sharing—it is too soon to tell. In the interim, and in the absence of legislative measures, the private sector and government should work together to scale-up some of the industry- and region-specific information-sharing practices now in place. The Financial Services Information Sharing and Analysis Center (ISAC) is a useful model.

ISAC, which was created in 1999, developed mechanisms for sharing information between the public and private sectors, and works closely with the Department of the Treasury and DHS as well as the Federal Deposit Insurance Corporation. Oil and gas companies already share information with each other and some are holding ad hoc discussions with the Federal Bureau of Investigation at the city and state level.[29] The discussions should be formalized and extended to include more companies, but they will be no substitute for oil and gas companies investing more money and energy in their own security.[30]

Washington also needs to shift strategy on the international front. The U.S. government has tried to establish a credible deterrent to future attacks, but the attribution problem—attacks can be masked and routed through multiple networks, making it difficult to identify who is responsible in a timely manner—make this an incredibly difficult technical task. In an October 11, 2012, speech in New York, Secretary of Defense Panetta suggested that the United States had made significant progress in creating a deterrent to cyberattacks, saying, "Potential aggressors should be aware that the United States has the capacity to locate them and to hold them accountable for their actions that may try to harm America." The threshold for "harm," however, remains undefined, and it is best that it remains ambiguous. While the United States is unlikely to respond to the theft of data from oil and gas producers with its own cyber- or kinetic attacks, a clear red line—e.g. death or extensive physical damage—may encourage hackers to operate just under the bar for an explicit U.S. response.

The Obama administration should also draw oil- and gas-producing states into cybersecurity discussions. Saudi Arabia has reportedly been in discussions with DHS to "set up a system where it can provide protection against cyberattacks."[31] The U.S. State Department has begun cybersecurity dialogues with China, India, Brazil, South Africa, and other countries, and has partnered with Kenya, Senegal, and Ghana to cohost cybersecurity and cyber-crime workshops. Similar efforts should be developed for the Gulf states and other oil and gas producers, and would include representatives from the U.S. State, Defense, Homeland Security, and Energy departments as well as oil and gas companies. The discussions would focus on broad issues of cyber crime and information sharing, incident response, computer forensics, and the development of national computer emergency response teams (CERTs).

In addition, information sharing between U.S. companies and their overseas operations needs to be simplified. Companies cleared to receive classified threat information must have effective and safe ways to get that information into the hands of the foreign nationals who maintain network security; this will require Washington to either provide clearance to greater numbers or to package the information to allow sharing while protecting intelligence assets. Deciding how broadly to share classified information is a complex and sensitive issue, but one that policymakers will have to confront to effectively combat cyber threats overseas.

CONCLUSION

The number and sophistication of attacks on U.S. oil and gas companies appears to be increasing. Likewise, their potential for inflicting damage on critical infrastructure is growing, with last year's Shamoon virus illustrating the growing potency of cyber threats. Creating widespread destruction or disruption still remains difficult, and is probably out of reach for all but sophisticated state-based or state-supported actors. But those capabilities will diffuse to others over time, and there are risks that a relatively unsophisticated attack could have a more widespread impact because of unexpected spillover effects.

Given the continued deadlock over domestic legislation, the most effective efforts will be self-help. Industry must find new ways to scale local efforts to share threat information. In addition, the United States should begin wide-ranging discussions with other oil- and gas-producing countries on cybersecurity.

About the Authors

Blake Clayton is fellow for energy and national security at the Council on Foreign Relations.

Adam Segal is the Maurice R. Greenberg senior fellow for China studies at the Council on Foreign Relations. An expert on security issues, technology development, and Chinese domestic and foreign policy, Segal currently leads the cyberconflict and cybersecurity initiative and is director of the Independent Task Force on U.S. Policy the Digital Age. His recent book, *Advantage: How American Innovation Can Overcome the Asian Challenge,* looks at the technological rise of Asia.

Endnotes

[1] Rachael King, “Virus Aimed at Iran Infected Chevron Network,” *Wall Street Journal*, November 9, 2012.

[2] William J. Lynn III, “Defending a New Domain: The Pentagon’s Cyber Strategy,” *Foreign Affairs* 89, no. 5 (September/October 2010), pp. 97–108; McAfee Foundstone Professional Services and McAfee Labs, “Global Energy Cyberattacks: ‘Night Dragon’,” White Paper, February 10, 2011, http://www.mcafee.com/us/resources/white-papers/wp-global-energy-cyberattacks-night-dragon.pdf; James Blitz, “MI5 Chief Sets Out Price of Cyberattack,” *Financial Times*, June 25, 2012; Camilla Hall and Javier Blas, “Qatar Group Falls Victim to Virus Attack,” *Financial Times*; and David E. Sanger, David Barboza, and Nicole Perlroth, “Chinese Army Unit Is Seen as Tied to Hacking Against U.S.,” *New York Times,* February 18, 2013.

[3] Definition adapted from Seymour M. Hersh, “The Online Threat: Should We Be Worried About a Cyber War?,” *New Yorker*, November 1, 2010.

[4] Zain Shauk, “Hackers Hit Energy Companies More Than Others,” FuelFix.com, March 25, 2013, http://fuelfix.com/blog/2013/03/25/electronic-attacks-hit-two-thirds-of-energy-companies-in-study/.

[5] Nathan Hodge and Adam Entous, “Oil Firms Hit by Hackers From China, Report Says,” *Wall Street Journal*, February 10, 2011.

[6] Interview with anonymous U.S. cybersecurity consultant.

[7] Rachael King, “Virus Aimed at Iran Infected Chevron Network,” *Wall Street Journal,* November 9, 2010.

[8] David Perera, “ICS-CERT Issues Search Engine and Exploit Tool Alert to Critical Infrastructure Operators,” FierceGovernmentIT, November 5, 2012, http://www.fiercegovernmentit.com/story/ics-cert-issues-search-engine-and-exploit-tool-alert-critical-infrastructur/2012-11-05#ixzz2E0c5YJko.

[9] Interviews with anonymous oil company executives and security consultants.

[10] Zain Shauk, “Malware on Oil Rig Computers Raises Security Fears,” Houston Chronicle Energy, February 23, 2013, http://www.houstonchronicle.com/business/energy/article/Malware-on-oil-rig-computers-raises-security-fears-4301773.php#ixzz2O01Ax21m.

[11] Nicole Perlroth and David E. Sanger, “New Computer Attacks Traced to Iran, Officials Say,” *New York Times*, May 24, 2013.

[12] For an overview, see Christopher Bronk and Eneken Tikk-Ringas, “The Cyber Attack on Saudi Aramco,” *Survival: Global Politics and Strategy* 55, no. 2 (April/May 2013), pp. 81–96.

[13] An earlier version, Stuxnet 0.5, was reportedly deployed in 2007 and surreptitiously closed valves in order to damage the Natanz uranium enrichment facility. Dan Goodin, “Revealed: Stuxnet “beta’s” Devious Alternate Attack on Iran Nuke Program,” *ArsTechnica*, February 26, 2013, http://arstechnica.com/security/2013/02/new-version-of-stuxnet-sheds-light-on-iran-targeting-cyberweapon.

[14] Warwick Ashford, “Stuxnet Hit Chevron’s Systems, the Energy Giant Admits,” ComputerWeekly.com, November 9, 2012, http://www.computerweekly.com/news/2240170737/Stuxnet-hit-Chevrons-systems-the-energy-giant-admits.

[15] Information from an anonymous reviewer with expertise in cybersecurity.

[16] “‘Shamoon’ Virus Most Destructive Yet For Private Sector, Panetta Says,” *Reuters*, October 11, 2012, http://www.reuters.com/article/2012/10/12/us-usa-cyber-pentagon-shimoon-idUSBRE89B04Y20121012.

[17] Interviews with anonymous U.S. cybersecurity specialist.

[18] “The lessons of Shamoon and Stuxnet ignored: US ICS still vulnerable in the same way,” *Infosecurity,* January 5, 2013, http://www.infosecurity-magazine.com/view/30058/the-lessons-of-shamoon-and-stuxnet-ignored-us-ics-still-vulnerable-in-the-same-way.

[19] Interview with anonymous U.S. cybersecurity expert.

[20] Josh Rogin, “NSA Chief: Cybercrime Constitutes the ‘Greatest Transfer of Wealth in History’,” The Cable, ForeignPolicy.com, July 9, 2012, http://thecable.foreignpolicy.com/posts/2012/07/09/nsa_chief_cybercrime_constitutes_the_greatest_transfer_of_wealth_ in_history.

[21] Zain Shauk, “Hackers Hit Energy Companies More Than Others,” FuelFix.com, March 25, 2013, http://fuelfix.com/blog/2013/03/25/electronic-attacks-hit-two-thirds-of-energy-companies-in-study.

[22] Mark Clayton, “Energy Sector Cyberattacks Jumped in 2012. Were Utilities Prepared?,” *Christian Science Monitor*, January 7, 2013, http://www.csmonitor.com/Environment/Energy-Voices/2013/0107/Energy-sector-cyberattacks-jumped-in-2012.-Were-utilities-prepared.

[23] Eric Byres, “Next Generation Cyber Attacks Target Oil and Gas SCADA,” *Pipeline & Gas Journal* 239 no. 2 (February 2012), http://pipelineandgasjournal.com/next-generation-cyber-attacks-target-oil-and-gas-scada.

[24] Christopher Bronk and Adam Pridgen, "Cybersecurity Issues and Policy Options for the U.S. Energy Industry," Baker Institute Policy Report no. 53, The James A. Baker III Institute for Public Policy of Rice University (September 2012).

[25] U.S. Department of Energy, "Energy Delivery Systems Cybersecurity," Energy.Gov, http://energy.gov/oe/technology-development/energy-delivery-systems-cybersecurity. Accessed May 2013. See also U.S. Department of Energy, "Roadmap to Achieve Energy Delivery Systems Cybersecurity – 2011," http://energy.gov/oe/downloads/roadmap-achieve-energy-delivery-systems-cybersecurity-2011.

[26] Office of the Press Secretary, "Executive Order--Improving Critical Infrastructure Cybersecurity," Press Release, The White House, February 12, 2013, http://www.whitehouse.gov/the-press-office/2013/02/12/executive-order-improving-critical-infrastructure-cybersecurity.

[27] Interview with several anonymous U.S. oil and gas executives who cover cybersecurity.

[28] Tiffany Kaiser, "Former CIA/NSA Head: Cyber Security Threats 'Horribly Over-Classified'," *DailyTech*, October 7, 2011, http://www.dailytech.com/Former+CIANSA+Head+Cyber+Security+Threats+Horribly+OverClassified/article22953.htm.

[29] Interviews with anonymous U.S. oil and gas cybersecurity specialist.

[30] For excellent resources on what companies can do to increase their cyber-related security, see the U.S. Business Roundtable's January 2013 report, *More Intelligent, More Effective Cybersecurity Protection*, as well as a host of free training materials, recommendations, and references available on the website of the U.S. Department of Homeland Security's Industrial Control Systems Cyber Emergency Response Team (ICS-CERT), accessible at http://ics-cert.us-cert.gov.

[31] Ellen Nakashima, "As Cyberwarfare Heats Up, Allies Turn to U.S. Companies For Expertise," *Washington Post*, November 22, 2012.