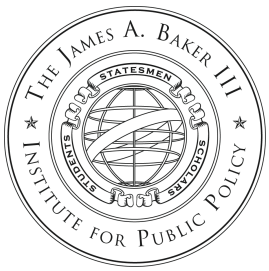

James A. Baker III Institute for Public Policy
Rice University

Working Paper

Hack or Attack?
Shamoon and the Evolution of Cyber Conflict

by

Christopher Bronk, Ph.D.

Fellow in Information Technology Policy
James A. Baker III Institute for Public Policy
Rice University

and

Eneken Tikk-Ringas, Ph.D.

Senior Fellow for Cyber Security
International Institute for Strategic Studies
Manama, Bahrain

February 1, 2013

This paper has been approved for publication in the March 2013 issue of
Survival, Global Politics and Strategy

Introduction

On August 15, 2012, the Saudi Arabian Oil Company (also known as Saudi Aramco), Saudi Arabia's national petroleum concern, a producer, manufacturer, marketer and refiner of crude oil, natural gas, and petroleum products,[1] was struck by a computer virus that possibly spread across as many as 30,000 Windows-based personal computers operating on the company's network. According to news sources, it may have taken Aramco almost two weeks to fully restore its network and recover from a disruption of its daily business operations caused by data loss and disabled workstations resulting from the incident. Computer security research community dubbed the virus reputed to have spread across Aramco's network Shamoon.

While reports of a virus on a major multinational firm's computer network is not a rare event, an incident against a company that holds so much of the world's spare oil production capacity is not a non-issue. Saudi Aramco is critical to the world's petroleum markets. The world's largest oil producer, it reportedly holds 10 percent of global supply and its crude production may stand above 13 percent of the global total, with sales amounting over $200 billion annually.[2]

The Shamoon outbreak likely affected the operation of Personal Computers (PCs) inside Aramco, with the malicious software's main function being the indiscriminate deletion of data from computer hard drives. Although there was no apparent oil spill, explosion or other major fault in Aramco operations, the incident impacted production and business processes of the company as at least some drilling and production data were likely lost.[3] Shamoon was also found to have propagated to the networks of other oil and gas firms, including that of RasGas, a joint venture of Qatar Petroleum and US-based ExxonMobil.

---

[1] Headquartered in Dhahran, Saudi Arabia, the Saudi Arabian Oil Company manages the world's largest proven conventional crude oil and condensate reserves of 259.7 billion barrels and ranks among world's top refineries and natural gas liquids exporters. Established in 1933 and owned entirely by the Government of Saudi Arabia since 1980, this corporation represents a bundle of strategic business interests. Until 1945 the enterprise was named Californian Arabian Standard Oil Company and the conglomerate still holds subsidiaries and affiliates in the United States, the Netherlands, UK, China, Japan and Singapore. Saudi Aramco, www.saudiaramco.com.

[2] Stanley Reed, "The World's Most Influential Companies," *Bloomberg*, http://images.businessweek.com/ss/08/12/1211_most_influential/8.htm.

[3] John Roberts, "Cyber threats to energy security, as experienced by Saudi Arabia," *Platts*, November 27, 2912, http://blogs.platts.com/2012/11/27/virus_threats/#comments

The Shamoon-Aramco incident comes after years of warning about the risk of cyber attacks against critical infrastructure. Protection of the Saudi petroleum infrastructure from military and terrorist attack has been a common concern for the US and Saudi Arabian governments for decades. Iran presents a potentially significant threat to petroleum facilities in Saudi Arabia's Eastern Province.[4] Even a partial disruption of these production facilities would have an immediate impact on oil supplies and prices, with knock-on effects for the global economy.

Although the Shamoon attack did not result in any physical damage to critical infrastructure in the Middle East, there has been a secondary impact on risk assessment for providers of critical services worldwide. The incident has raised serious security concerns between the United States and Iran. US Defence Secretary Leon Panetta referred to Shamoon as "'very sophisticated,'" and "raising 'tremendous concern about the potential for the use of that kind of tool'" and by noting that "there are only a few countries in the world that have that capability,"[5] thus keeping the incident in the political and media spotlight. For this reason, we sought to document the Shamoon case and consider its impact on broader policymaking regarding the Middle East, energy and cybersecurity issues.

The following study will cover the background and context of the Shamoon incident, itemize open-source facts and public statements surrounding the episode.

Context

Saudi Aramco and Gulf Oil Production

The Persian Gulf remains a key area for global oil and gas production. Four of the world's top ten oil producers, Saudi Arabia, Iran, Iraq and the United Arab Emirates ship all or much of their production via tankers through the Straits of Hormuz. Including Kuwait (the world's eleventh largest oil producer), some 22 million barrels of oil are produced in the region daily.[6] Production of natural gas is also significant, with Qatar standing as the world's second largest exporter in the

[4] Joshua Izkowitz, Shifrinson and Miranda Priebe, "A Crude Threat: The Limits of an Iranian Missile Campaign against Saudi Arabian Oil," *International Security* 36 (2011): 167-201.
[5] Leon Panetta, "Defending the Nation from Cyber Attack," (New York, NY, October 11, 2012), Business Executives for National Security, http://www.defense.gov/speeches/speech.aspx?speechid=1728.
[6] *Key World Energy Statistics*, International Energy Agency, 2012.

commodity. Although unconventional oil and gas production methods, including shale gas and oil extracted from tar sands, are transforming the global energy market, exports of oil and gas from the region will remain a fundamental piece of the global supply for the foreseeable future. Consumers in Europe and Asia remain highly dependent upon oil supplies from the Arabian Peninsula, Iraq and Iran.

The primary target of Shamoon, Saudi Aramco, is a leading player in the petroleum industry. In December 2006, the Financial Times titled Aramco "the world's biggest company."[7] Research conducted by the FT and McKinsey estimated Aramco's worth to be close to $781bn market capitalisation. Again in 2010, the FT made similar assertions regarding Aramco's market value, concluding that "Aramco alone would command a value of $7 trillion, 40 times Shell's market capitalisation."[8] These numbers make Aramco's worth substantially higher than publicly traded oil companies. However, the fact that Aramco is a nationally owned firm makes it harder to verify these market valuations.[9] As with most Saudi-owned enterprises, Aramco has adopted a multi-layered hierarchical power structure since the Saudi government took full control of the company in 1980 by acquiring 100 percent stake.

Aramco's corporate management is made up of a president, six vice-presidents and a non-Saudi general counsel who serves as the corporate secretary. The board of directors and corporate management report regularly to the Supreme Council for Petroleum and Mineral Affairs (SCPM), a body established in January 2000. "The creation SCPM created a body in charge of all matters related to petroleum, gas, and other hydrocarbon affairs in onshore and offshore areas."[10] It shoulders the task of managing all affairs of petroleum, gas and other hydrocarbon

[7] Francesco Guerrera and Carola Hoyos, "Saudi Aramco revealed as biggest group," *Financial Times*, December 14, 2006, http://www.ft.com/intl/cms/s/0/0ea4c450-8bb1-11db-a61f-0000779e2340.html#axzz2Dtm5R2it.
[8] "Big Oil, bigger oil," *Financial Times*, February 4, 2010, http://www.ft.com/intl/cms/s/3/c5b32636-116f-11df-9195-00144feab49a.html#axzz241yHCicp.
[9] Sheridan Titman, "What's the Value of Saudi Aramco, *Texas Enterprise*, February 9, 2010, http://www.texasenterprise.utexas.edu/article/whats-value-saudi-aramco
[10] Anthony Cordesman, *Saudi Arabia Enters the Twenty-First Century: The Military and International Security Dimensions*, Praeger: Westport, Conn., 2003, p. 328.

materials in Saudi Arabia. Physical security for Aramco infrastructure and operations is a foremost concern to forces under the Saudi interior ministry and military.[11]

Physical protection of Saudi Aramco's infrastructure is likely of keen interest to the company's leadership. After a foiled terrorist attack on the massive petroleum processing complex at Abqaiq in 2006, concern regarding the vulnerability of the company's infrastructure rose.[12] Since Abqaiq, Aramco has worked with the US experts and companies on its contingency planning and security solutions. In physical security, Aramco has likely acquired significant capability and was recognized for its efforts by the American Society of Industrial Security in 2010.[13] Cyber security at Aramco, and in the entire region, is largely an unknown, however.

ICT and Cyber Capabilities in the Gulf

The Gulf States have invested heavily in their information and communications technology (ICT) infrastructure in the past decade. ICT spending in the GCC reached $33 billion in 2007, 50 percent above than the global average.[14] Spending between 2011 and 2015 is forecast to total $318 billion by 2015 due to increased demand for ICT in public institutions, healthcare, construction, oil and gas and telecommunications.[15] Where other regions of the planet have seen ICT investment slow as technological penetration tops out in relation to population, the Middle East remains an area of enormous growth.

ICT penetration in the Middle East varies widely but there is a general global correlation between wealth and ICT penetration. Saudi Arabia runs against the grain to some degree. With a population of 26 million, there are estimated to be fewer than 9 million Internet users despite

[11] Anthony Cordesman and Nawaf Obaid, *Saudi Petroleum Security* (Working Draft), Center for Strategic and International Studies: Washington DC, November 2004.
[12] Khalid al-Rodhan, "The Impact of the Abqaiq Attack on Saudi Energy Security," *Saudi-US Relations Information Service*, February 28, 2006, http://www.susris.com/articles/2006/ioi/060228-rodhan-abqaiq.html.
[13] "Security Recognized for Professionalism," Saudi Aramco, accessed January 19, 2012 http://www.saudiaramco.com/en/home/news/latest-news/2010/security-recognized-for-professionalism.html#news%257C%252Fen%252Fhome%252Fnews%252Flatest-news%252F2010%252Fsecurity-recognized-for-professionalism.baseajax.html.
[14] Karim Sabbagh, Ramez Shehadi and Shant Okanyan, "Next-Generation ICT Parks Bridging the GCC Technology Gap," Booz & Company, 2009, http://www.doz.ae/images/stories/files/Next_Generation_ICT_Parks_Booz%20&%20Co.pdf.
[15] "GCC ICT: Being Part Of An Increasingly Digital World," *Markaz Research*, October 23, 2011, http://www.markaz.com/DesktopModules/CRD/News_Single.aspx?ikey=456&Module_IKey=32

high per capita GDP figures. Statistics for Iran, a country of 78 million, are somewhat lower relative to population, with about 8 million Internet users.[16] What both countries, and the rest of the region share is a meteoric rise in the growth of mobile telephone and smart phone connectivity.

While there has been no significant lack of investment in computing and telecommunications in the countries of the Gulf Cooperation Council (GCC), cross-GCC ICT efforts are generally facilitated by foreign firms. National ICT strategies are limited by the still embryonic nature of national visions to develop ICT capabilities. In addition, the GCC is yet to develop a sophisticated lattice of regulatory instruments to support a sustainable information society. The need for developing local ICT expertise is vital as GCC relies heavily on foreign workers with a short cycle of knowledge through acquisition, representing a counterproductive policy hindering ICT becoming the integral and indigenous component of GCC economic development.

Despite these shortcomings, the Gulf States have made investments in ICT and information resources. Qatar, with a population of less than 2 million, has built the Al Jazeera satellite television news network into a globally recognized brand for Middle East news content and Dubai has worked to create an innovation hub in its Dubai Internet City project. There are, however, significant issues for information control in the region as well, especially in the wake of the revolutions of the Arab Spring.

The region's cyber warfare capabilities, held by both states and non-state actors in the region, are subject to speculation. Offensive and defensive cyber preparedness is difficult to assess with great granularity, however, a number of factors are useful in formulating rough capability. Such an index should include technological infrastructure items as considered above, as well as indices of talent, such as educational capacity in science, technology, engineering and math (STEM) fields as well as more focused capabilities in computer and information sciences that align with cyber security proficiency.

[16] The 8 million Internet users is via the *CIA World Factbook*. Some years ago, the Iranian government sought to restrict high-bandwidth connections to the general population, generally prohibiting connections with speed greater than 128 kilobits per second for non-commercial users. See: Robert Tait, "Iran bans fast Internet to cut west's influence," *The Guardian*, October 17, 2006.

Then the question becomes "How good are the hackers?" This can be only the roughest of assessments.[17] The United States, Russia, China, and Israel are generally considered to hold robust and significant offensive and defensive cyber capabilities. Several Western European countries — Germany, the United Kingdom, and France — likely hold strength as well.[18] This is large part due to the strength of their signals intelligence services as well as the computational education establishments from which they recruit.

Perhaps the best publicly available indicator of relevant capabilities in the Gulf region is the number of citizens from each country holding advanced degrees in computer science, electrical engineering and information science. There is a yawning gap in computing between Iran and almost any other country in the region. Many Iranians pursue postgraduate education in computing, many of them abroad, and many of those individuals choose to remain abroad. Lebanese, Palestinians and Egyptians are notable in the field as well.[19] The Gulf States are not yet producing such talent, while Iran is, revealing an asymmetry of capability in domestically produced or foreign educated domestic talent. This asymmetry will likely require a decade or more of significant investment for the GCC countries to erase. These countries may be able to buy cyber defense capability, but enlisting foreign nationals to engage in cyber intelligence or offensive cyber operations poses serious dilemmas. The cyber overlay of the Gulf security picture suggests great immaturity among all players, but a definite intellectual lead held by Iran.

Regional and International Relations

Since the collapse of the Shah of Iran in 1979, regional tensions in the Persian Gulf have been a foremost international concern. The Soviet invasion of Afghanistan, the Iran hostage crisis, Iran-Iraq War, Israel's bombing of the Iraqi nuclear power station at Osirak, the Gulf 'tanker war,' and two US-led military campaigns against Saddam Hussein's Iraq culminating in nearly a

[17] Namosha Veerasamy, Marthie Grobler, and Basie von Solms, "Towards a Cyberterrorism Life-Cycle (CLC) Model," *Proceedings of the 4thWorkshop on ICT Uses in Warfare and the Safeguarding of Peace 2012 (IWSP 2012)*, School of Management, IT, and Governance, University of KwaZulu-Natal and Defence, Peace, Safety and Security Council for Scientific and Industrial Research, Sandton, South Africa, August 16, 2012.
[18] Chris Bronk, "Between War and Peace: Considering the Statecraft of Cyberspace," in *The Secure Information Society: Ethical, Legal and Political Challenges,* Jörg Krüger, Bertram Nickolay and Sandro Gaycken, eds., Springer: London, 2012.
[19] Consider, for example the contribution of Egyptian-born Taher Elgamal, one of the world's leading cryptographers.

decade of counterinsurgency and the extensive counter-terror operations aimed at Al Qaeda and its confederates indicate the acute security concerns in the region.

Continuing strains in regional relations have gathered around the Iran's influence in Shia political movements extending to the Levant and the Iranian nuclear program. Regional tensions were only exacerbated by the emergence of the massive Arab Spring protest movement, extending from North Africa to the Arabian Peninsula and disrupting traditional power structures. Not to be ignored in the revolutions of 2011 is the role of cyberspace as an avenue for political organization, dissent and disruption.

Relations across the Gulf went into a deep freeze after the Iranian Revolution of 1979. Saudi Arabia along with the rest of the Gulf Cooperation Council states fear of Iranian interest in "exporting the revolution" and empowering Shiite communities living outside of Iran. Sectarian tensions escalated following the "Arab Spring" with protests erupting in Bahrain, a critical ally of the US and Saudi Arabia, and Syria, which has strong historic relations with Iran. US and Western presence in the Gulf has also contributed to the deterioration of relations between Iran and GCC states. Iran views the GCC's security and military dependence on Western powers as an extension of western imperial dominance in the region.[20]

US-Iranian relations remain poor, with the two countries engaging in open conflict in 1988, as the US retaliated against Iranian attacks on shipping and the mining of the Gulf. No official relations have existed between the countries since the US broke all diplomatic relations after the seizure of its embassy and its staff by Iranian students. Hostility between the two states has been further aggravated by Iran's nuclear and ballistic missile programmes as well as Iran's sponsorship of US identified terror groups. Interestingly, the US government de-listing the anti-regime Mojahedin-e-Khalq (MEK) as a terror group in September 2012, while some allege that the US covertly supported the group in its assassination campaign against Iran's nuclear scientists.[21]

[20] "Iran Majlis condemns merger of KSA, Bahrain," *PressTV*, May 14, 2012, http://www.presstv.ir/detail/2012/05/14/241177/iran-raps-saudi-plans-bahrain-merger/.
[21] Seymour Hersh, "Our Men in Iran," *The New Yorker*, April 6, 2012, http://www.newyorker.com/online/blogs/newsdesk/2012/04/mek.html.

Although the United States declared in a declassified digest of a 2007 National Intelligence Estimate that Iran's production of nuclear weapons was not imminent, it continued to voice opposition to the Iranian government's position on everything from uranium enrichment to the movement of IED technologies to Iraq's insurgency. The 2009 Iranian elections, protests, and crackdown further deepened the wedge between Iran and the United States. With Iran's bellicose statements toward Israel and support for Hezbollah, relations between Tehran and Washington had reached a bitter low by the time Barack Obama arrived in the White House.

The US Government prohibits almost all trade with and investment in Iran and has mounted sanctions that largely block investment in the petroleum sector, supply of commercial products and importation of most Iranian goods. While sanctions initially were levied during the 1979 hostage crisis, in recent years the US and international sanctions have tightened due to Iran's nuclear program. The Comprehensive Iran Sanctions, Accountability, and Divestment Act of 2010 threatened punitive action against firms doing business with Iran, particularly in the energy sector.

In addition to US efforts to isolate Iran, the United Nations has levied additional sanctions against the country, regarding its nuclear program, most recently with UN Security Council Resolution 1929. Punitive measures contained within the resolution include: prohibition of ballistic missile development, a ban on military equipment sales and other military assistance to the country, an extensive travel ban for listed individuals, and a freezing of assets held by the Iranian Revolutionary Guards and the national shipping line.

Also relevant are the measures undertaken on the financial front both by the US government and transnational bodies. The US Treasury Department's Office of Foreign Assets Control has barred a number of Iranian banks from accessing the US financial system, some due to their ties with Hezbollah, an organization labeled a terror group by the US State Department.[22] Financial sanctions have also come from other quarters, with the European Union's expression of displeasure regarding Iranian nuclear enrichment manifested in the Society for Worldwide

[22] "U.S. imposes sanctions on Iranian bank," *People's Daily*, September 9, 2006, http://english.peopledaily.com.cn/200609/09/eng20060909_301143.html.

Interbank Financial Telecommunication (SWIFT) "expelling as many as 30 Iranian financial institutions — including the Central Bank — crippling their ability to conduct international business and further isolating the country from the world economy."[23] These measures have left Iran increasingly isolated, the Iranian economy cratered, and the rial plummeting in value. While the US secretary of state would not draw a straight line from international sanctions to the dire economic situation, she offered this prescription. "Of course the sanctions have had an impact as well, but those could be remedied in short order if the Iranian government were willing to work with the P5+1 [the five security council members plus Germany] and the rest of the international community in a sincere manner."[24] The economic lever of sanctions has undoubtedly had an impact in Iran's security stance, but beyond sanctions we must also consider the cyber elements directed against it.

Cyber Conflict and Shamoon

Stuxnet and the Middle East Balance of Power

In the autumn of 2010, reports surfaced of a new piece of malware rapidly propagating across the Internet, but with concentrations of the virus in the .id (Indonesia), .in (India) and .ir (Iran) national level domains of the Internet.[25] After discovery by a security team in Belarus, antivirus companies began publishing analyses of the self-replicating malware worm, which was dubbed Stuxnet. As additional analysis was conducted on the Stuxnet worm, its sophistication became apparent. It included a number of previously unknown weaknesses in the Microsoft Windows operating system, known in the security community as zero day exploits.[26] In addition, Stuxnet contained instructions for the Siemens programmable logic controller (PLC), a type of computer employed in supervisory control and data acquisition (SCADA) systems found in power plants, production lines, and other heavy industry applications.

---

[23] Rick Gladstone and Stephen Castle, "Global Network Expels as Many as 30 of Iran's Banks in Move to Isolate Its Economy," *New York Times*, March 15, 2012.
[24] Julian Pecquet, "Clinton: Iran's leaders, not US, to blame for sanctions as country hit by protests," *The Hill*, October 3 2012, http://thehill.com/blogs/global-affairs/middle-east-north-africa/260077-clinton-extends-a-hand-as-protests-wrack-iran.
[25] Nicolas Falliere, Liam O. Murchu, and Eric Chien, *W.32 Stuxnet Dossier*, Symantec, February 2011.
[26] A zero day exploit is a previously unknown vulnerability in a computer application or operating system that allows an unauthorized party access to a computer system.

Stuxnet is a highly sophisticated piece of malware. Its delivery system, which allowed for its eventual worldwide propagation, included not less than three previously unknown exploit vectors for the Microsoft Windows operating system (known as zero-day exploits). But even greater sophistication was found in Stuxnet's payload, designed to alter the operations of Siemens Simatic process logic controller (PLC) computers. Stuxnet was designed to monitor PLCs, infect them by inserting new instructions and then "mask the fact that a PLC is infected."[27]

Hypotheses regarding Stuxnet's target and capabilities circulated widely, but primarily focused on Iran. Details emerged that Stuxnet had likely affected Iran's nuclear program, including the major uranium enrichment facility at Natanz.[28] Stuxnet appeared to subvert the computers employed to run the centrifuges employed in the enrichment process. At the same time reports surfaced from Iran of covert action directed against its nuclear scientists, at times with deadly results.[29] Rumors swirled in the global hacker community that Iran was willing to pay hefty fees to security analysts willing to root out Stuxnet and secure the Iranian cyber infrastructure, but clear attribution of Stuxnet, like most other cyber incidents was difficult to achieve.[30]

This changed when New York Times reporter David Sanger published an account of the covert program in which Stuxnet was created in his chronicle of the Obama national security doctrine in June 2012. Sanger alleged that the US had initiated a major cyber attack program directed against the Iranian nuclear program under the name Olympic Games.[31]

Sanger made the argument, based on the statements of unnamed sources in the US intelligence and national security apparatus that the US needed to embrace action beyond mere sanctions to retard the progress of the Iranian nuclear program. He asserted,

[T]hese questions ultimately led to the creation of one of the most secret, compartmentalized programs inside the US government. The details of 'Olympic Games' were known only by an

[27] Nicolas Falliere, Liam O Murchu, and Eric Chien, *W32.Stuxnet Dossier*, Ver 1.4, February 2011, Symantec, 36.
[28] Christopher Williams, "Barack Obama 'ordered Stuxnet cyber attack on Iran'," *The Telegraph*, June 1, 2012.
[29] David Sanger, *Confront and Conceal: Obama's Secret Wars and Surprising Use of American Power*
[30] Mark Clayton, "Stuxnet malware is 'weapon' out to destroy ... Iran's Bushehr nuclear plant?" *Christian Science Monitor*, September 21, 2010. See also, Ralph Langner, *Robust Control System Networks: How to Achieve Reliable Control after Stuxnet*, Momentum: New York, 2012.
[31] Sanger, *Confront and Conceal.*

extremely tight group of top intelligence, military and White House officials. The intent of the operation was twofold. The first was to cripple, at least for a while, Iran's nuclear progress. The second, equally vital, was to convince the Israelis that there was a smarter, more elegant way to deal with the Iranian nuclear problem than launching an airstrike that could quickly escalate into another Middle East war, one that would send oil prices soaring and could involve all the most volatile players in the region.[32]

Sanger further posits:

This was exactly the vulnerability that nuclear experts and computer engineers inside the United States and Israeli governments decided to try to exploit in 2007 and 2008. What if they could somehow secretly take command of the specialized computer controllers that run the sprawling centrifuge plant at Natanz? What if they could implant some code that would lie dormant for weeks or months, waiting for a chance to wreak havoc? And what would happen if one day, when the Iranians thought everything was running smoothly, the code would kick in to order those centrifuges to speed up too quickly or slow down too fast, creating exactly the kind of instability that sometimes happens naturally? And how long would it take the Iranians to figure out that someone, somehow, had gotten inside their systems?[33]

Following Stuxnet, reports of cyber action against Iranian assets continued to emerge. Russia's Kaspersky, a major antivirus firm, brought to light the discovery of Flame – a complex piece of malware initially titled Skywiper by the CrySyS Lab at the Budapest University of Technology and Economics due to its capacity to delete computer hard drives.[34] Kaspersky, the CrySyS Lab and the Iranian national computer emergency response team (CERT) announced the discovery of Flame jointly, with the International Telecommunications Union apparently having served as a facilitator for connecting the Iranians with European malware analysis talent.[35] Flame had reportedly been detected on the computer systems of Iran's primary oil facility at Kharg Island in

[32] Ibid.
[33] Ibid.
[34] sKyWIper Analysis Team, *sKyWIper (a.k.a. Flame a.k.a. Flamer): A complex malware for targeted attacks* (v. 1.05), Laboratory of Cryptography and System Security, Budapest University of Technology and Economics, May 31, 2012.
[35] Ellen Messmer, "Iran's discovery of Flame malware turning into political hot potato," *Network World*, May 30th, 2012, http://www.networkworld.com/news/2012/053012-iran-flame-malware-259708.html.

the Persian Gulf.[36] While it is unclear as to what, if any, damage Flame did to Iranian oil and gas production, its discovery provides evidence that cyber attacks against Iran had spread beyond the nuclear program into the lifeblood of its economy, its energy sector.

More than two years after Stuxnet was discovered in Natanz, it reportedly re-surfaced in Iran, however it is unknown if this was a new effort or just the latest identification of the program.[37] Stuxnet did contain instructions to cease replicating after June 24, 2012.[38] Although it is difficult to assess the exact damage Stuxnet caused to the Iranian nuclear program it is likely that the delay in uranium enrichment is less significant as the Iranian capability to boost up their cyber capabilities, both defensive, and as Shamoon might prove, offensive.

Cyberspace and the Global Oil and Gas Market

When we consider the window of vulnerability via the cyber vector there are important questions regarding how information and computing technologies impact the operations of producers of oil and gas. Oil production is an enormously technology intensive activity. The complexity of offshore oil and gas operations is frequently compared with that of space exploration, due to the forbidding nature of bringing to the surface deposits thousands of feet underground and under water.

With the rise of oil prices over the last decade has come the economic impetus to develop unorthodox means of production. Higher oil prices have made drilling in deeper water or extraction from the tar sands of Alberta or elsewhere economically viable. This is well understood. Less so is the importance of computational innovation in oil and gas exploration and production. Modeling and analysis of seismic data has led to an ever-increasing need for massive supercomputing resources. The size and power of these computers is noteworthy as evinced by coverage of Russia's Gazprom. A 2011 industry news piece claimed the company, "needs an

[36] Darren Pauli, "Iran CERT fingers Flame for oil refinery attacks," *SC Magazine*, May 30, 2012, http://www.scmagazine.com.au/Tools/Print.aspx?CIID=302718.
[37] "Neuer Angriff mit Stuxnet," Neue Zürcher Zeitung, December 25, 2012, http://www.nzz.ch/aktuell/international/iran-meldet-neuen-angriff-mit-computervirus-stuxnet-1.17909054
[38] William Jackson, "Stuxnet shut down by its own kill switch," *GCN*, June 26, 2012, http://gcn.com/articles/2012/06/26/stuxnet-demise-expiration-date.aspx

HPC-system for seismic data processing and reservoir simulation. If the system is deployed, it is likely to be amongst the most powerful supercomputers in the world."[39] Gazprom is not alone, with BP recently announcing its intent to construct an 110,000 square foot supercomputing facility at its US headquarters as part of a $100 million investment in high-performance computing.

Supercomputing is not the only area in which oil and gas firms have made significant investment. Upstream operations, in which unrefined oil and gas are tapped and moved to refining, have also incorporated a growing computational component.[40] Offshore platforms, wellheads, and pipelines are now digitally interconnected with a plethora of sensors and process control computers feeding information directly back to corporate operations centers at corporate headquarters around the globe. As with almost any other finished product, the supply chain for petroleum has grown lean, efficient, and globally interconnected thanks to ICT. Furthermore, seismic data collected in costly exploration activities has long been viewed as an intellectual crown jewel of the industry. With the migration of these seismic data to computerized modeling and study, new protection issues emerge.

At the same time that an infrastructure of highly industry specific computing has been deployed in oil and gas, the industry has also adopted many of the same technologies as other multi-national firms including personal computers, smart phones, and globe-spanning high-speed computer networks. Energy executives do business with the same off-the-shelf technologies as those in other sectors, and information security shops in those companies are tasked with securing digital storage and communications to the highest degree possible, accepting the limitations of security for the rapidly evolving IT ecosystem that encompasses modern corporate business operations.

---

[39] "Oil and Gas Giant Considers Petascale Supercomputer," *HPCwire*, July 11, 2011, http://www.hpcwire.com/hpcwire/2011-07 11/oil_and_gas_giant_considers_petascale_supercomputer.html.

[40] "Microsoft Maximizes Upstream Operations Agility and Control," Microsoft, 2010, https://www.google.com/url?sa=t&rct=j&q=&esrc=s&source=web&cd=17&ved=0CGUQFjAGOAo&url=http%3A%2F%2Fdownload.microsoft.com%2Fdownload%2FC%2FF%2FE%2FCFE4502F-B04D-43F4-B7BE-35CAA29539B6%2FOil_Gas_Upstream%2520Operations.pdf&ei=FTbTULaSKYrV2QX7xoGABg&usg=AFQjCNE1Nwdc2IMgpevHbzhTWQ645YUK4Q&sig2=DzUL8lyJEyyjRGOpXHkdVw&bvm=bv.1355534169,d.b2I.

Players in the oil and gas industry probably harbour concerns about three major cyber security issues: (1) theft of intellectual property (IP) such as designs, plans or other strategic information; (2) conduct of cyber-espionage aimed at short-term decision-making in business activities; and (3) conduct of disruptive events from the deletion of data to the manipulation of computer systems involved in the production and refining of petroleum.[41] In addition, the energy industry must cope with cybersecurity concerns that are generic to all operators of IT, the cyber hygiene activity of protecting from general malware and cybercrime concerns, as well as industry specific threats to both information resources and infrastructure.

The Oil & Gas Cybersecurity Threat Space

Attack/Malware Issues	Vulnerabilities & Targets
General Concerns (Viruses, Phishing, Fraud, etc.)	Information Issues (Theft of data, coordinated cyber espionage)
Specific Concerns (Targeted attacks, Spearphishing, customized malware, insider complicity)	Infrastructure Issues (Business computing disruption, critical infrastructure attacks)

Then there comes the question of who might wish to perform each of the types of cyber incident described above. Theft of IP and eavesdropping of internal communications might be of value to both industrial competitors and governments as well as state run national oil companies (NOCs). Disruption might attract other parties, from hacktivist organizations, possibly aligned with radical environmentalist groups to terror groups and hostile foreign powers or their proxies. We can surmise that different types of actors are able varying degrees of resourcefulness and capacity in performing cyber operations. That said, pulling off a noteworthy cyber operation may only carry a cost in the hundreds of thousands or millions of dollars.

[41] Chris Bronk and Adam Pridgen, *Baker Institute Policy Report #53 – Cybersecurity Issues and Policy Options for the U.S. Energy Industry*, Baker Institute for Public Policy, September 2012.

How well Aramco or any other energy company is performing in cybersecurity is hard to assess. Even the most technologically astute firms in the software industry, exemplified by Google and Microsoft, have been on the receiving end of significant penetrations of their enterprise networks. Further, these are companies that invest heavily on cyber security (but also have very high public profiles, making them significant targets as well). Gene Spafford's consideration of the security topic (lumped in with its companion issue, privacy) probably speaks to a consensus view of the problem. "Security and privacy are not always treated as first-order problems. Things are deployed and made widely available without regard for security and privacy. In a best-case scenario, security and privacy are thought of as add-ons. Worst case, they're ignored completely."[42]

Oil and gas companies operating in the Middle East may likely find a growing cyber component to consider in the overall picture of above ground concerns. Internal political upheaval, terrorism, interstate conflict and the influence of non-regional powers will all impact the calculus of security there. That the security equation will include a significant and growing cyber component over the next decade is a virtual certainty as long as cyber attacks produce results and cannot be easily foiled, avoided or attributed.

The Shamoon Virus

On August 15, 2012 at 11:08am Saudi-Arabian time, a self-replicating computer virus enabled an unknown person or persons to commence overwriting files on the hard disks of about 30,000 Windows-based workstations belonging to Saudi Aramco. Shamoon's primary function was to delete data on computer hard drives. The virus acquired the name Shamoon in the malware analysis community due to a string of a folder name within the malware executable.[43] Also named W32.Disttrack, Shamoon corrupts files on a compromised computer and overwrites the MBR (Master Boot Record) in an effort to render a computer unusable. Propagation of Shamoon appears to have been pseudo-random in nature, rather than designed to target the work stations of particular Aramco employees.

[42] "Fast track to the future: The 2012 IBM Tech Trends Report," *IBM Center for Applied Insights*, December 2012, http://public.dhe.ibm.com/common/ssi/ecm/en/xie12346usen/XIE12346USEN.PDF.
[43] That string is: "C:\Shamoon\ArabianGulf\wiper\release\wiper.pdb".

According to Symantec, W32.Disttrack consisted of several components. The Dropper refers to the main component and source of the original infection and a number of other modules dropped or copied into the infected computers. The Wiper module was responsible for the destructive functionality of the threat and the Reporter module was accountable for reporting infection information back to the attacker.

After having been released from one of the workstations on the company's internal network, Shamoon, designed by its creator(s) to activate at a specific time, overwrote files with a fraction of an image of a burning American flag, then instructed the compromised computers to report their infection back to an IP address.[44] Some have commented that insertion of the al-Shamoon virus required someone who had physical access to a computer on the Aramco network.[45] This obviously raises concerns about the implementation of the company's cyber and physical security measures.

As with other significant cyber incidents, the firms, independent analysts and government agencies of the malware analytic community began releasing preliminary assessment within days of initial report regarding Shamoon's detection. The US Department of Homeland Security's computer emergency readiness team (US-CERT) assessed the volatility of the Shamoon malware in late August.

Because of the highly destructive functionality of the Shamoon "Wiper" module, an organization infected with the malware could experience operational impacts including loss of intellectual property (IP) and disruption of critical systems. Actual impact to organizations vary, depending on the type and number of systems impacted.[46]

Seculert described Shamoon as a two-stage attack in which the attacker first took control of an internal machine connected directly to the Internet, and used that machine as a proxy to the

[44] Nicole Perlroth, "Connecting the Dots After Cyberattack on Saudi Aramco," *The New York Times*, August 27, 2012. http://bits.blogs.nytimes.com/2012/08/27/connecting-the-dots-after-cyberattack-on-saudi-aramco.
[45] Jeffrey Carr, "Was Iran Responsible for Saudi Aramco's Network Attack?" *Digital Dao*, http://jeffreycarr.blogspot.com/2012/08/was-iran-responsible-for-saudi-aramcos.html.
[46] United States Computer Emergency Readiness Team, "JSAR-12-241-01—Shamoon/DistTrack Malware," Joint Security Awareness Report, August 29, 2012, http://www.us-cert.gov/control_systems/pdf/JSAR-12-241-01.pdf

external Command-and-Control (C2) server. After initial deployment, other internal machines were infected. Then the Shamoon malware was executed to wipe all evidence of other malicious software or stolen data from those machines. The proxy was then used again to report back to the external C2, a capacity dismissed as broken by others.[47]

Moscow-based Kaspersky, a major vendor of anti-virus software, issued report on Shamoon as well, noting in particular, the amateurish errors included in the virus. Kaspersky analyst Dmitry Tarakanov's frankness is typical of the tone found in the community of those who study malware. Regarding Shamoon's capacity to report back to those who created it, Tarakanov is dismissive.

[I]n reality, this part of the Shamoon communication module does not work at all. This is because an author made another silly error (in addition to flawed date comparison). The author intended to create full path to the file ?filer<random number>.exe using ?sprintf function, where it should have been used the format string:

"%s%s%d.%s with following parameters: Windows folder string, "\Temp\filer" string, random number and "exe" string relatively.

But instead of mentioned correct format string, the malware writer used ?%S%S%d.%s with an uppercase ?S. This causes a ?sprintf function failure and no full path string is created. Lack of full path means that no file is dropped. No file, no execution. So, the Shamoon malware does not have a functionality to execute other programs.[48]

Saudi Aramco was able to restore all its main internal network services by August 26, reporting it had cleaned all the workstations that were impacted, and resumed normal business.[49] The attack must have caused considerable disruption to the activities of the Saudi Arabian Oil

[47] "Shamoon, a two-stage targeted attack," *Seculert*, August 16, 2012, http://blog.seculert.com/2012/08/shamoon-two-stage-targeted-attack.html
[48] Dmitry Tarakanov, "Shamoon The Wiper: further details (Part II)," *SecureList*, September 11, 2012, http://www.securelist.com/en/blog/208193834/Shamoon_The_Wiper_further_details_Part_II
[49] "Saudi Aramco repairs damage from computer attack," *Al Arabiya*, August 26, 2012, http://english.alarabiya.net/articles/2012/08/26/234372.html.

Company as the incident necessitated a significant downtime period for the company's public facing website. Downtime of Saudi Aramco websites was noted even after the company publicly announced full recovery from the consequences.[50] It is also likely that most of infected computers were rendered temporarily unusable due to an element in malware designed to overwrite the Master Boot Record. We assume that there was a non-trivial disruption to the business operations at Aramco in the response period to Shamoon, but the energy industry's more significant question is as to whether Shamoon impacted oil production in the Kingdom.

Aramco CEO Khalid al-Falih stated of the attack on the company's Facebook page, "We addressed the threat immediately, and our precautionary procedures, which have been in place to counter such threats, and our multiple protective systems, have helped to mitigate these deplorable cyber threats from spiraling."[51] Further, there has been no report of Shamoon reaching industrial control system (ICS) computers of the sort that would be involved in drilling or refining operations at Aramco or anywhere else. If true, this highlights an important lesson for oil and gas companies regarding the vital need for segmentation between computer systems responsible for general business operations and those employed in monitoring and controlling their upstream and downstream operations. Shamoon did, however spread beyond the boundaries of the initial point of delivery and onto the networks of other companies. Platts reported impact well beyond Aramco alone, claiming,

[b]oth drilling and production data were lost, including data provided by such drilling companies as Santa Fe, Ocean and Schlumberger ... The virus hit the company's management offices throughout the Kingdom. It also hit its offices in Houston and The Hague … It also hit the state-of-the art Exploration and Petroleum Engineering Center – Advanced Research Center in Dhahran, which is responsible for the company's upstream oil and gas technology development.[52]

---

[50] "Saudi Aramco restores network services," Saudi Aramco, http://www.saudiaramco.com/content/www/en/home/news.html#news%257C%252Fen%252Fhome%252Fnews%252Flatest-news%252F2012%252Fsaudi-aramco-restores-network.baseajax.html.

[51] "Saudi Aramco investigating origins of 'Shamoon' virus following attack," Al Arabiya, September 12, 2012, http://english.alarabiya.net/articles/2012/09/12/237530.html.

[52] John Roberts, "Cyber threats to energy security, as experienced by Saudi Arabia," Platts, November 27, 2912, http://blogs.platts.com/2012/11/27/virus_threats/#comments.

Explaining the impact, Platts noted the enormous volumes of data involved in petroleum exploration and extraction mentioned above and the potential for polluted data reaching beyond the boundaries of Aramco's network.

Drilling produces enormous volumes of data, which is then transferred to a Saudi Aramco data base center and filtered, with other data discarded. The filtered data is supposed to be manually backed up twice a day but, perhaps because it was Ramadan, there were no backups carried out for either drilling or production data. It's the filtered data that's important…and it's the filtered data that was lost.[53]

Others observed Shamoon's spread to Qatar's Rasgas natural gas company, a joint venture between Qatar Petroleum and ExxonMobil, in late August.[54] With the impact of Shamoon felt inside Saudi Arabia and the Gulf states, discussion the virus has grown politicized. Secretary Panetta referred to Shamoon as a "'very sophisticated tool [a point refuted by Russia's Kaspersky] … rising 'tremendous concern about the potential for the use of that kind of tool' and that 'there are only a few countries in the world that have that capability.'" He also called it, "one of the first [pieces of malware] that can actually take down and destroy computers … to the point that they had to be replaced." [55] Symantec stated, "Threats with such destructive payloads are unusual and are not typical of targeted attacks."[56] However, memories long enough will remember the prognostications of digital doom forecast for the 1992 Michelangelo virus, which John McAfee considered a grave threat to millions of computers.

Due to the efforts of the malware analysis community in analyzing Shamoon's source code, we now understand a good deal of what happened, and perhaps even more about how it happened. Where large gaps of knowledge or contention remain is in why Shamoon happened and who did it.

---

[53] Ibid.
[54] Robert Tuttle, "Virus Shuts RasGas Office Computers, LNG Output Unaffected," *Bloomberg*, August 30, 2012, http://www.bloomberg.com/news/2012-08-30/virus-shuts-rasgas-office-computers-lng-output-unaffected-1-.html.
[55] Leon Panetta, "DOD News Briefing with Secretary Panetta and Gen. Dempsey from the Pentagon," October 25, 2012, U.S. Department of Defense, http://www.defense.gov/transcripts/transcript.aspx?transcriptid=5143.
[56] "The Shamoon Attacks," *Symantec Official Blog*, Symantec, August 16, 2012, http://www.symantec.com/connect/blogs/shamoon-attacks.

Attribution of Shamoon

Although a previously unknown group called "The Cutting Sword of Justice" has taken responsibility for the Shamoon incident, several questions about the real motivation and perpetrator remain. An 'anti-oppression hacker group' has publicly taken responsibility for the attacks, including posting blocks of I.P. addresses of thousands of Aramco PCs online as proof of the attack.[57] The group labeled itself as, "fed up of crimes and atrocities taking place in various countries around the world, especially in the neighboring countries such as Syria, Bahrain, Yemen, Lebanon, Egypt and … also of dual approach of the world community to these nations, want to hit the main supporters of these disasters by this action."[58]

Since Secretary of Defence Panetta voiced concern regarding Iranian cyber capabilities, thinking has focused on the connection between Shamoon and the reputed Olympic Games cyber attacks directed against Iran. Speculation on Shamoon has largely focused on Iran due to the increasingly tense regional geopolitics of the Persian Gulf region. Sanctions against Iran have grown increasingly difficult on the country. Iran is faced with the frightening prospect of bringing production offline, and due to the antiquated and decrepit state of the national oil and gas infrastructure, restoring production later under sanctions will doubtlessly be a daunting or at least expensive prospect.[59]

Iran has several competing incentives to move into the cyber domain in attempting to harm Saudi Arabia through its primary economic resource. In the face of trade sanctions, Iranian oil sits unsold on supertankers unable to find market while Saudi Arabia is producing 10 million barrels of oil per day. There are, of course, other factors that could be germane to an Iranian decision to employ a cyber attack against Aramco.

India, a longtime buyer of Iranian oil, sent an important signal when on July 20, 2012, India's Mangalore Refinery & Petrochemicals Limited, "bought Azeri, Saudi and Emirati crude to

[57] "Daily Report: How Aramco Got Hacked," *The New York Times*, October 24, 2012, http://bits.blogs.nytimes.com/2012/10/24/daily-report-how-aramco-got-hacked/.
[58] The Cutting Sword of Justice's full attribution may be found online at the file upload site PasteBin: http://pastebin.com/HqAgaQRj.
[59] Fareed Mohamedi, "The Oil and Gas Industry," *Iran Primer*, U.S. Institute for Peace, http://iranprimer.usip.org/resource/oil-and-gas-industry.

replace imports from Iran in July 2012 and it may halt purchases from Tehran altogether as sanctions make shipments more difficult."[60] As the sanctions have increasingly squeezed the Iranian economy, the country's leaders have responded with threats to close the Strait of Hormuz if sanctions weren't revoked. Of course, the same threat has been made before and Iran has not attempted to interfere with maritime traffic in the Persian Gulf. (To uphold its presence in the region and send a stabilizing signal to world energy markets, the US Navy sailed multiple carrier strike groups into the Persian Gulf despite the Iranian threat.) With direct military action a likely pyrrhic prospect at best, Iran is likely inclined to play the cyber card.

The pattern cyber action by proxy is in line with Iranian employment of proxy organizations to engage in terror attacks against the United States and its allies. Iran has consistently supported terror organizations, most notably Hezbollah, for decades. With terror attacks more effectively thwarted by the Saudis on their own soil since the low mark of attacks undertaken by Al Qaeda on the Arabian Peninsula on the US consulate general in Jeddah 2005 and attacks against expatriate compounds elsewhere, violent direct action by proxy is likely a harder feat to accomplish. In particular the failure of the February 24, 2006 truck bombing at the massive Abqaiq oil production facility resulted in much enhanced security measures. This, along with the relative quiet from the Kingdom on the terrorism front since, suggest that Saudi Arabia is a much harder terror target than it once was.

Thus, we consider a much less risky and more likely form of retribution for Iran sponsorship at arm's length of a damaging network attack against Saudi Aramco through a proxy like the Arab Youth Group.[61] It is difficult to conclude that Iran had nothing to do with the Shamoon incident. As indicated by James Lewis, it is implausible the Iranian government would not be aware of a major cyber operation consuming significant bandwidth and coming from sources inside in a country monitoring the Internet for political purposes would draw attention.[62] As a nation harmed by cyber attack, it makes sense that Iran would develop intrinsic cyber capabilities and

[60] "India's top buyer of Iran oil turns to Azeri, Saudi," *Reuters*, July 16, 2012, http://www.reuters.com/article/2012/07/16/india-mrpl-idUSL6E8IGAGO20120716.
[61] Jeffrey Carr, "Who's Responsible for the Saudi Aramco Network Attack?" Infosec Island, August 29, 2012, http://www.infosecisland.com/blogview/22290-Whos-Responsible-for-the-Saudi-Aramco-Network-Attack.html
[62] "U.S. says Iran behind cyber attack in Saudi Arabia," El Arabiya, October 13, 2012, http://english.alarabiya.net/articles/2012/10/13/243475.html.

employ them as it has employed other forms of clandestine force when direct attribution is not desired.

Iran has officially denied any part in the construction or deployment of Shamoon. Mehdi Akhavan Beh-Abadi, director of the Iranian National Center of Cyberspace stated of US official discussion regarding Shamoon, "We interpret this issue politically and in light of domestic issues and election in the United States."[63] That Shamoon occurred in an enormously sensitive region is important. Kaspersky analyst Roel Schouwenberg, from the company's Boston office considered, "If Shamoon happened in Norway, we wouldn't have been drawing these comparisons."[64] But even if Shamoon or something like it had impacted Norway's national oil company Statoil, it would be troubling nonetheless. Shamoon is important because it impacted Saudi Arabia, but also because of its placement in the oil and gas sector in general.

With regard to international security regime, there are important issues with which to contend on attribution and the role of proxies in cyber that have come into play because of Shamoon. In the event that the accusations about Iranian involvement are borne out the incident raises a serious question about pursuit of national interests via state or proxy actors against critical infrastructure. With only rather vague leads regarding Shamoon, it adds to the already long list of cyber incidents raising national security concerns but with no clear or credible attribution, thus further feeding the suspicions that there is no good cure for cyber security unless we can fix the issue of attribution.

Attribution, however, is a term of many facets. The architecture of computer networks indeed allows a degree of anonymity that combined with ill will and sufficient skills in hiding one's traces will make it difficult to identify the perpetrator. The highest (and most referred to) burden of attribution is applied in the domain of cyber crime where an act or an omission needs to be linked to a person without reasonable doubt. When it comes to state-on-state attribution and the

[63] "Iran denies U.S. claims it was behind Persian Gulf cyber attacks," *Tehran Times*, October 14, 2012, http://www.tehrantimes.com/politics/102372-iran-denies-us-claims-it-was-behind-persian-gulf-cyber-attacks.
[64] Michael Riley and Eric Engleman, "Malicious Code in Aramco Cyber Attack Suggests Lone Culprit," *Washington Post*, October 25, 2012, http://washpost.bloomberg.com/Story?docId=1376-MCFA4J0D9L3501-7O74U9ELP64SALGOFCOI56RJFE.

responsibility for state for non-state actors under its jurisdiction, different attribution requirements apply.

When it comes to state-on-state response or an event like Shamoon, the decision about sufficiency and qualification of evidence lies with Saudis. Like Estonia in 2007, Saudi Arabia is free to cooperate with other states to filter and weigh evidence, but any countermeasures would require a combination of compelling evidence, political will and response capability. Little practice can be found in the area of holding states responsible for cyber affairs and as in the case of applying the existing law of armed conflict to cyber, state responsibility in this field is still to be restated.

In case the target or victim country decides not to act, there is little that the international community can do other than noting the incident and speculating about its causes, course of action and consequences. Therefore, cases like Estonia 2007, Georgia 2008, Stuxnet and Shamoon leave us with more questions than answers.

In case the analysis about Iranian involvement is inaccurate, the need is reiterated for confidence-building among nations to avoid misappropriation and escalation of conflict as well a general duty to cooperate by governments of states whose jurisdiction is involved in either launch or routing of the attacks. If and how Shamoon or something like it could be viewed as requiring or justifying military response speaks to the grand problem of cyber security and the contested lines between war and mere acts of belligerence or bellicosity.

Policy Implications on Protecting Critical Infrastructures: Due Diligence & Risk

Political incentives behind and within cyber attacks have made targeting of critical infrastructure providers real. Companies are being targeted by specific political attacks, and the attacks are becoming increasingly frequent and costly.[65] Shamoon is a reminder that enterprises need to be alert about the possibility of becoming the target of a politically motivated cyber incident. For

[65] "Symantec 2010 Critical Infrastructure Protection Study Global Results," Symantec, October 2010, http://www.symantec.com/content/en/us/about/presskits/Symantec_2010_CIP_Study_Global_Data.pdf.

major oil exporters, production and distribution infrastructures are critical infrastructures, a term generally referring to systems and assets vital to the functioning of states and societies.[66] Increasingly, information technology and Internet Protocol based networks form part of how critical infrastructure and services are designed, maintained and provided.[67]

Protecting the information technology components of critical infrastructure became a wider subject of discussion on an international level at the wake of this millennium. In May 2003 the G8 Justice & Interior Ministers adopted Principles for Protecting Critical Information Infrastructures. At the end of the same year the UN Second Committee processed an almost identical text into a UN General Assembly Resolution.[68] An EU Directive followed in 2008.[69] NATO has also emphasized the protection of critical infrastructure as an important aspect of emerging security challenges.[70]

Yet international policy does not provide much actionable guidance without a layer of national legal drafting to set the minimally required standards, due diligence criteria and auditing or reporting mechanisms that help deter and mitigate incidents. Discussion on cyber security often turns on the willingness of the companies to work with national governments to determine who should protect information systems and assets and how this should be done. In supporting the functions of a critical infrastructure companies, careful scrutiny is needed in the balance upon which public-private partnership between government and business regarding commitments in securing critical services and systems.

---

[66] According to Article 2 (a) of Directive 2008/114/EC 'critical infrastructure' means an asset, system or part thereof located in Member States which is essential for the maintenance of vital societal functions, health, safety, security, economic or social well-being of people, and the disruption or destruction of which would have a significant impact in a Member State as a result of the failure to maintain those functions. The US has defined CI as systems and assets, whether physical or virtual, so vital to the United States that the incapacity or destruction of such systems and assets would have a debilitating impact on security, national economic security, national public health or safety, or any combination of those matters (42 USC § 5195c - Critical infrastructures protection).

[67] Chris Bronk, "A Governance Switchboard: Scalability Issues in International Cyber Policymaking," *Cyber Dialogue 2012: What is stewardship in Cyberspace?* University of Toronto, March 2012, http://bakerinstitute.org/publications/ITP-pub-BronkCyberDialogue2012-031312.pdf.

[68] A/RES/58/199. Creation of a global culture of cybersecurity and the protection of critical information infrastructures.

[69] Directive 2008/114/EC as of December 8, 2008 on the identification and designation of European critical infrastructures and the assessment of the need to improve their protection. Available at: http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2008:345:0075:0082:EN:PDF

[70] "The Protection of Critical Infrastructures," NATO Parliamentary Assembly, 2007 Annual Session, http://www.nato-pa.int/Default.asp?SHORTCUT=1165.

Related to the Shamoon case, there are serious and concrete consequences to classifying a service or entity as critical, both from national and international perspective. Qualifying an object or activity 'critical' raises specific questions about required (and imposed) security standards that become relevant (and are costly) for the purposes of developing and implementing security solutions in relevant enterprises and processes and redefines the relationship of industry with governments, international organizations, and often with their customers.

It is not clear if the mere fact of belonging to a critical industry makes the whole enterprise critical and whether being categorized critical in one jurisdiction has any direct consequences to affiliates and processes extending to other jurisdictions. Saudi Aramco is a massive entity with over thirty subsidiaries and affiliates around the world. While Aramco leadership asserts that production was unaffected,[71] there are important questions from the Shamoon case germane to other players in oil and gas, and elsewhere in industry. But the critical point for policy is how government, commercial actors, the international system and other players share and manage cyber incident risk. Shamoon identifies just how broadly a major cyber attack can impact key national capabilities and concerns.

When a particular function is deemed a critical infrastructure protection (CIP) item, corporations are no longer necessarily sole stakeholders. In CIP, governments traditionally share a burden of defense or at least coordination of defenses. There is a fine line between governmental and private effort in protecting critical infrastructure entities and indeed conflicting views as to how much outside protection (interference) is needed and what is considered sufficient protection. A fundamental question is to what degree government can require or provide protection to enterprises whose stability and well being is vital for national interests and security. Conversely, there is the important question, raised most recently by the sophisticated DDoS attacks against US banking institutions, as to how the state should intervene in protecting corporate interests from covert cyber action undertaken by other states.[72]

[71] Matthew Schwartz, "Saudi Aramco Restores Network After Shamoon Malware Attack," *Information Week*, August 27, 2012, http://www.informationweek.com/security/attacks/saudi-aramco-restores-network-after-sham/240006278.
[72] Ellen Nakashima, "Banks seek NSA help amid attacks on their computer systems," *Washington Post*, January 11, 2013, http://articles.washingtonpost.com/2013-01-11/world/36272281_1_banks-ddos-nsa

Developing working public-private partnerships in CIP is a challenging task as it requires very careful consideration by government of relevant business goals and processes as well as appreciation of the governmental threat assessment logic and required supervisory steps by the private sector. It raises practical questions as to how to organize state level guidance and supervision, especially in sectors where strong supervision and coordination has already occurred with regard to other areas of public policy, e.g. money laundering in the banking sector or personal data protection in health care.

Although the need for public-private protection and defence models has been acknowledged, the policy goals and business routines are difficult to marry without resistance. A plan of action for achieving a working CIP model will therefore need to have regard to a balanced and considered role division. When it comes to technical security, few governments can effectively add to the expertise already existing in the private sector and specific companies. At the same time, public and semi-public authorities such as computer emergency response teams (CERTs) and crisis management entities hold capabilities for coordinating threat assessment and mitigation efforts and assess defenses required from strategic security perspective.

Additionally, it may prove useful to revisit the existing security policies to specify the relationship and hierarchy of security requirements that apply to critical infrastructure (CI) or critical information infrastructure (CII) providers. In regulating security, several legal regimes existed before the emergence of CI concerns that may be useful. For example, the European data protection requirements impose a general requirement of technical, organizational and physical security to all computers on which personal data is processed, and require such security measures to take into account process-specific risks.[73]

Cyber attacks against CI are unlikely to go unnoticed and therefore an appropriate response is in order. This raises the questions of strategic communications, decision-making about who and how responds to which aspects of the incident. Such transgressions challenge national security

[73] "Commission proposes a comprehensive reform of the data protection rules," European Commission, January 25, 2012, http://ec.europa.eu/justice/newsroom/data-protection/news/120125_en.htm.

and raise the questions of use of force considered by lawyers of international conflict.[74] Therefore, responses to CI cyber incidents matter from both national authority and general deterrence perspective and, in the light of the Aramco-Shamoon incident, require special attention by enterprises, governments and international organizations alike

Epilogue and Trend Indicators

From a purely technical perspective, the Shamoon aka W32.Disttrack malware did not add much new to the cyber threat landscape. While it undoubtedly incapacitated a significant number of Saudi Aramco's Microsoft Windows computers, the degree to which the company's bottom line was impacted seems to be fairly minimal. The full impact of Shamoon on Aramco simply is not publicly known. There is more to the incident though. Those who see the Aramco incident designating a new development in hacktivist behavior may well be mistaken.[75] Indeed, most known episodes of Lulzsec and Anonymous attacks have mainly rested on Distributed Denial of Service or defacement, but it is questionable if the proxies behind the Aramco virus were that loosely organized.

In Shamoon, someone applied a degree time and effort. If we accept the American inference, Iran is one of the obvious suspects. Targeting infrastructure critical not only for the Saudi economy, but also global economy and security and not likely being affected by the outcome itself. Iran's holding a fundamental disagreement with most of the international community about the oil embargo against it and also about the nature of its own nuclear activities and being one of the very countries in possession of the Wiper code makes Iran a perfect suspect.

Of course, Iran denies any involvement. In international political cyber attacks this is not new. Russia never admitted to a role in the cyber attacks leveled against Estonia in 2007 nor the cyber attacks during the Russo-Georgian War in 2008. Similarly, China has categorically denied the widespread cyber espionage complaints leveled against it. If we accept that Shamoon was

[74] Oona A. Hathaway, Rebecca Crootof, Philip Levitz, Haley Nix, Aileen Nowlan, William Perdue, and Julia Spiege, "The Law of Cyber Attack," *California Law Review* 100 (2012): 817-886, http://www.californialawreview.org/assets/pdfs/100-4/02-Hathaway.pdf.
[75] Perlroth, "Connecting the Dots After Cyberattack on Saudi Aramco."

physically delivered to the Aramco network by a human agent then that raises an interesting set of questions. Ostensibly, such an agent may be found. Was it a mole inside Aramco? A break-in? The compromise of a laptop? We may never know.

In case the accusations about Iranian involvement are correct the incident raises a serious question about pursuit of national interest via state or proxy actors against critical infrastructure. This is worrisome, as objects that were vulnerable only to fairly overt mechanisms of attack may now be harmed by clandestine, cyber actions. Was Shamoon yet another element of cyber covert action to be added to the repertoire of Iran's non-avowed clandestine, often violent, activities? Or perhaps it was mere signaling or as James Lewis has suggested, part of a larger grudge match between the Kingdom of Saudi Arabia and the Islamic Republic of Iran.

What is for sure is that Shamoon is another disquieting development in the development of cyber conflict. In cyber there is a dividing line between those events we imagine to be possible and those we know to be. Shamoon adds another item in our inventory of known cyber events, but does nothing to set limits on what we consider to be possible. In short, the deployment of Shamoon against the largest oil and gas company on the planet has made the world a more dangerous place. In cyberspace we see ample reason for concern and grossly insufficient effort at stabilization and confidence building between nations and other parties.

Acknowledgments

The authors would like to thank a number of colleagues for their helpful comments and contributions in the drafting of this paper including Roger Hurwitz, James Lewis, Greg Rattray, Art Conklin, Dan Wallach, Cody Monk, Adam Pridgen, Mika Kerttunen, Nigel Inkster, Joseph Nye, Wafa Al Sayed and Islam Al Tayeb.