Saudi Aramco: The Existence of Cyber War

Submitted by: xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx

Military and Strategic Studies – ITSC201-ISS

Professional Communications and Presentation Skills – COMM256-ISS

Southern Alberta Institute of Technology

Submitted to: Dr. Stuart White PhD & Karen Riley MEd.

November 26, 2019

Abstract

This essay is an exploration on the cyber attack of the company Saudi Aramco by means of the virus Shamoon. It explains in detail what happened, what the ramifications were, and the economic and political fallout. The research focused on understanding the relationship between Saudi Arabia and Iran and the importance of the infrastructure to the country. Once the analysis of the attack is completed, a thorough and comprehensive comparison to the classical thinkers will transpire. The classical thinkers that these theories will be drawn upon are: Carl von Clausewitz, Sun Tzu, Julian Corbett, and Niccolo Machiavelli. The implications to cyber warfare are boundless; this has been shown through the numerous attacks that have happened in the past (e.g. Stuxnet, Flame, Duku, etc.) mainly targeting critical infrastructure. The research and evaluation will lead to a better understanding of the Saudi Aramco cyber attack and the perpetual effects that still exist today.

Keywords: Shamoon, Saudi Aramco, Cyber Attack, Cyber war

Saudi Aramco: The Existence of Cyber War

When Saudi Aramco employees went to bed on the night of August 14, 2012 it would have never occurred to them that they would be waking up to an influx of problems created by a computer virus. Although there had been major attacks on infrastructure previously, Aramco was not prepared for the disastrous effect that the Shamoon virus would have on not only their technology, but also in the oil distribution around the world. When investigating Saudi Aramco and its significance, the concepts brought forth by major classical thinkers such as: Sun Tzu, Carl von Clausewitz, Niccolo Machiavelli, and Julian Corbett are considered heavily as this helps elucidate why the attack may have happened and what the attackers may have been trying to achieve. David Sanger (2018) quipped, "Cyber operations around the world are broad, ranging from espionage and destructive malware – the kind that could knock a whole country back into the analog age (36)". Noting this, an attempt will be made to enlighten and delve deeper into the understanding of cyber warfare and the importance of protecting critical infrastructure.

What Happened and Why

On the morning of one of Islam's holiest evenings, August 15, a massive strategic cyber attack was executed against one of the world's most valuable companies, Saudi Aramco. The Saudi State owned and publicly funded enterprise was targeted on this day as most of its employees were absent for the Lailat al Qadr celebrations. As discovered by reading Blanches (2012) article, the attack consisted of a virus worm infection, now referred to as Shamoon, which spread to over 30,000 computer systems eradicating and overwriting every file with malice. At 11:08, somebody with 'authorized' company access initiated the attack. It was successful in erasing data on three quarters of Aramco's systems while replacing files with images of a burning American flag. Aramco was forced to shutdown its internal networks in an attempt to

prevent the virus from spreading any further, which had been accelerated by employee emails and internet access. The virus was programmed to report a newly infected computer's address back to one centralized infected local computer, as means to demonstrate and collect how far the infection was spreading. Aramco had a bit of 'luck' to the design of their systems, as their resource production system and internal networks were not tied to one another, ensuring that only data and data systems were affected. It wasn't long before the virus was contained and the reverse engineering of its signature could begin. Security experts enumerated that the attack would have had to come from a physical attack vector, executed by a privileged employee, or employees, by executing a malicious file or simply inserting a USB thumb drive into a computer on the network. The internal network was closed, and the infected addresses were still being released to the public, further supporting the notion that an internal privileged employee of Aramco was involved. As experts dove into the source code of Shamoon, they noticed a coincidental naming of the function that erased memory, named 'Wiper'. This was the same name of the function code that erased data in the Flame attack on Iran discovered in May. As Blanche (2012) had stated; "now that we've done it to the Iranians - who are quick learners - what is to stop them modifying sophisticated computer worms for use in their own cyber warfare and doing it back to us." This raised early suspicion that this attack wasn't a coincidence and was possibly even retaliation.

Espionage and Sun Tzu

Cyber attacks allow for extremely quiet, destructive, and most importantly, widespread attacks on a system. Viruses, like Shamoon, encapsulated many of Sun Tzu's ideas and even without the same technology, the methodologies still remain relevant. The use of espionage is key to infiltration and the deployment of viruses. Sun Tzu (1994) noted five types of spies: local,

internal, enemy spies or double agents, expendable spies, and living spies (189). Of these five categories, Shamoon could be considered two different types – living and local. With the need to gather adequate intelligence from internal spies, it would then be accurate to state that Shamoon embodied a local spy because it was intended to report to an external server (Mackenzie, 2012). As noted, gaining and understanding intelligence is a key aspect of an operation, and it is unknown how long it took to gather and implement this information.

The total number of computers that were affected by the virus was vast (Abokhodair & Dehlawi, 2013, IEEE). The process to infect such a substantial quantity of computers began with a malicious executable that was enabled by Saudi Aramco employees. Once the executable was activated, the attackers gained access by compromising computers and ultimately spreading the virus further. The Shamoon virus was placed onto the network it started to work in three phases. Firstly, the dropper determined what it had access too, replicated and embedded itself, then finally self-spreading through the network. Secondly, the wiper was programmed to initiate on August 15th. When the program ran it destroyed the data, and sent a report about the destroyed data . Lastly, it would run a reporter module which would send information back to the central computer (Mackenzie, 2012). A virus that can destroy data and report about it is essentially a local spy, a living spy, and it is a spy you can entirely trust. The virus in essence also turns the employees unknowingly into your own spy.

Machiavelli and The State

The design of the Aramco Board of Directors, and the inclusion of foreign allies, was a foundational way of creating manipulative control on the state but also generating perceivable corruption. Just as Machiavelli (1992) examined, “For whoever has thoroughly fortified his town, and put himself on such a footing with his subjects.... will always be attacked with much

circumspection (27)". As seen on Aramco's website (Saudi Aramco, 2019), the Board of Directors have primarily been compiled of members who hold government positions such as; Governor of Public Investment Fund, Saudi Minister of Finance, General Authority of Tax, General Authority of Statistics, Vice Chairman of the UN Global Compact and Global Compact Foundation. The remaining part is made up of members from international companies; The Chevron Phillips Chemical Company, Director of Baker Hughes (a General Electric company), and Managing Director for Royal Dutch Shell. Collectively, based on this design and the information known about the Board of Directors, Machiavelli (1992) would have argued that,

> A prudent Prince should follow a middle course, by choosing certain discreet men from among his subjects, and allowing them alone free leave to speak their minds on any matter on which he asks their opinion, and on none other. But he ought to ask their opinion on everything. (63)

If Aramco was to have followed this notion of Machiavellian teaching, there is potential they could have avoided the accusations of corruption from the people. The creation of the Board of Directors, including members from outside nations with vested involvement in local and state industry, creates a stronger level of presence and an increase of invested interest to remain in control. With having members of government hierarchy, especially ones directly related to public finance and statistical information, are in a total position of power for exerting direct manipulation over the populace in the forms of information and monetary understanding, which are implemented with personal agenda. As Machiavelli (1992) stated,

> When you see a Minister thinking more of himself than of you, and in all his actions seeking his own ends, that man can never be a good Minister or one that you can trust.

> For he who has the charge of the State committed to him, ought not to think of himself (62).

From this, it can be said that corruption is not hard to develop when private agendas involve public monies. The motives behind the attacks have been directed towards removing and disrupting "tyranny and oppression" (Cutting Sword of Justice, 2012), and it does not take more than examining the Board of Directors for Saudi Aramco and reflecting on Machiavelli, to understand why there were, and still are, people who feel this way.

Limited Objectives, Friction, and Clausewitz

Carl von Clausewitz's theories of limited objectives and friction are pertinent to the ideas surrounding Shamoon and its destruction. Not only did it affect the company on a grand scale but it according to AFP, "…an August cyber attack on its computer network targeted not just the company but the kingdom's economy as a whole" (2012). It is a fitting claim that the Cutting Sword of Justice (CSOJ) attempted to cause as much havoc within the company as possible. Shamoon was meant to have catastrophic effects, and although it is not considered as refined as virus' such as Stuxnet, it is meant to achieve total cyber warfare (Zhioua, 2013, IEEE Conference). The concept behind releasing the Shamoon virus is one that appears well thought out and developed. The success from the CSOJ came from Clausewitz's (1976/2007) notion that the understanding of friction and obstacles faced, as well as the cognizance that things will go wrong was a critical aspect of cyber warfare (67). Unfortunately for the CSOJ, the attempted cyber attack may have been intended to be more absolute, in that it would completely shut down the company and therefore the countries oil production, but in fact it ended up unintentionally being a limited objective. The home state can ultimately become more powerful as the enemy's resources are targeted and destroyed (Clausewitz, 1976/2007, 258). Since Aramco had two

separate networks, the company inadvertently protected itself from a total war objective. The outcome that Shamoon had on the economy came down to oil distribution being halted. This was momentous as Saudi Aramco was the largest oil producer in the world. Fortunately, due to oil production and exploration being on a different network, it was one less piece of the puzzle for Aramco to worry about (AFP, 2012).

When considering the centre of gravity in the Saudi Aramco case, the oil infrastructure seems most prevalent. Through the evaluation of important industries, the government, and the civilian population, it appears that the oil industry is the hub of all power and movement where everything depends (White, 2019). This was clear as the destroying of Aramco affected international relationships and product distribution throughout the world. The fog of war is considerable in this circumstance. Aramco had increased their spending towards cyber security throughout 2012, but it is not clear whether the CSOJ was aware of this attempt at defensive tactics (Alshathry, 2017, 3039). The Cutting of Sword of Justice never divulged which state or company (if any) they belonged too, but it is reasonable to imagine that passions may have had a part in the attack. If there are passions expressed by the attacking state, there is likelihood that the war will be accelerated (White, 2019).

Continued Thoughts

The primary goal of this attack was disruption. Although the ultimate strategy was never known, or the source of the attackers never confirmed, the instability that resulted from it was the desired effect. It is easy to think of Corbett (1911) in this instance, and when he stated "Whether our immediate object were to bring the enemy's main fleets to action or to exercise economic pressure, it made but little difference (101)". The plan was to create ultimate economic and political disruption, and it did. The estimated financial damage was in the order of

$388 billion USD (Abokhodair & Dehlawi, 2013). The lack of security infrastructure that Aramco had, and their characterization as being corrupt, because of the involvement of the Saudi Regime, made it a rich target for attackers. As Corbett (1911) noted, the sturdiest defence is needed in the strongest attacks (261). As was discussed earlier, the lacking development of Aramco's security was sub par, and in turn, it could be potentially held responsible for the ability of this type of attack to manifest. By attacking Aramco, the largest of Saudi industrial and economic providers, coupled with the political involvement in the company hierarchy, can ultimately be seen as a limited attack on the Saudi Regime. As the CSOJ (2013) said,

> One of the main supporters of this disasters is Al-Saud corrupt regime that sponsors such oppressive measures by using Muslims oil resources. Al-Saud is a partner in committing these crimes. Its hands are infected with the blood of innocent children and people.

By directly attacking a fundamental commodity such as oil, and disrupting the economic stability, they are ultimately creating a strategic blockade for international trade and involvement. The most plausible reasoning for the attacks can be gathered from Corbett's concept that the best way to acquiesce action, is to control the oppositions resources (101). This in turn led to financial upset and diplomatic instability. Because of this attack, a 12-day shut-down took place before Saudi Aramco was able to distribute effectively again (AFP, 2012).

Implications for Modern Day Cyber Security

Saudi Aramco is not only a prime target for attacks because of their high profits and political stances, but also because they publicly implied that they have a weak defense. Al-Saud had said that the kingdom of Saudi Arabia did not incentivise the research and development of their cyber security. Due to the interconnected alliance between Saudi Aramco and Al-Saud, not having security in one is equivalent to not having security in the other. Had Saudi Aramco embodied Sun Tzu by considering, "When [your objective] is nearby, make it appear as if

distant; when far away, create the illusion of being nearby" (39). If this were true this attack may have been thwarted. The public announcement of a company's weakness, is an open invitation for attacks on your system. Al-Saud declared that Saudi Arabia may require the United States or other foreign nations to step in and assist" (Abokhodair & Dehlawi, 2013). Security is a key aspect to large industries, where a failure in security can result in extreme losses, and flaws in any individual's security should be kept secret. Despite the importance of security, Saudi Aramco had put off financing a proper security team. Kubecka said, an attack of this magnitude on a smaller company, would have caused bankruptcy in pursuit of recovery. (Rashid, 2015).

After the attack experts analyzed the virus further. It is believed that the virus was written by amateurs, but it is also said that this was retaliation after the Stuxnet attack on Iran. Rob Rachwald described the attack as "the first hacktivist-style assault to use malware" (Leyden, 2012). He continues to explain that the most common attacks are denial-of-service, or any attacks that would attempt to disrupt service – which are not destructive in nature (Rashid, 2015). As recently as September of 2019, Saudi Aramco had another attack on their systems. Aramco then gained a reputation of responding poorly during conflict. They have characterized themselves as vulnerable, thus making them a greater target to future attacks.

Conclusion

When considering the affects that the Shamoon virus had on Saudi Aramco, it is apparent that not only is critical infrastructure important, but also that Aramco has not done enough to protect its assets. The CSOJ was able to infiltrate and plant a virus that was capable of destroying systems and eliminating crucial information. The significance of this attack is one that was comparable to the ideas of the four classical thinkers, Clausewitz, Sun Tzu, Machiavelli, and Corbett. All of these thinkers are closely linked to various – but important – aspects of the attack. The concepts ranged from espionage, to friction, to state control, and limited and

absolute war. Through an extensive investigation of the classical thinkers and the attack itself, one would then be able to understand how Shamoon was implanted, the effects it had on Saudi Aramco, and the implications that still exist today. Aramco has been a target multiple times and has yet to build a robust defence to eradicate potential cyber issues and protect its greatest resource, oil.

References

Abokhodair, N. & Dehlawi, Z. (2013, June 4-7). Saudi Arabia's response to cyber conflict: A case study of the Shamoon malware incident. *2013 IEEE International Conference on Intelligence and Security Informatics (ISI).* doi: 10.1109/ISI.2013.6578789

AFP (2012, Dec 9). *Saudi Aramco says August cyber attack targeted entire country.* Retrieved November 19, 2019 from https://www.securityweek.com/saudi-aramco-says-august-cyber-attack-targeted-entire-country

Alban, K. & Kessem, L. (2017, Feb 15) *The full Shamoon: How the devastating malware was inserted into networks.* Retrieved on November 19, 2019 from https://securityintelligence.com/the-full-shamoon-how-the-devastating-malware-was-inserted-into-networks/

Alshathry, S. (2017, Feb) Cyber attack on Saudi Aramco. *International Journal of Management and Information Technology, 11*(5), 3037-3039. Retrieved from https://pdfs.semanticscholar.org/6a0e/dae9946d64eef4450328d08a5cc38340a1a3.pdf

Blanche, E. (2012, Dec). Cyber wars. *Middle East, 438*. pg 12-17. Retrieved on November 26, 2019 from https://eds.b.ebscohost.com/eds/detail/detail?vid=0&sid=0d86ddd7-7db5-4185-a67a-b31bcc748ada%40sessionmgr101&bdata=JnNpdGU9ZWRzLWxpdmUmc2NvcGU9c2l0ZQ%3d%3d#AN=84310345&db=f5h

Brock, C., & Pridgen, A. (2010). Cybersecurity issues and policy options for the U.S. energy industry. *Baker Institute Police Report, 53,* 1-15. Retrieved from https://www.bakerinstitute.org/files/628/

Clausewitz, C. (2007) *On war* (M. Howard & P. Paret Trans., B. Heuser Ed.) New York NY: Oxford University Press. (Original print 1976).

Corbett, J. (1911). *Principles of maritime strategy.* London: Longmans.

Cutting Sword of Justice. (2012, Aug 15). Pastebin: *Anyonymous.* Retrieved on November 26, 2019 from https://pastebin.com/HqAgaQRj

Machiavelli, N. (1992) *The prince.* (N.H. Thomson, Trans.). Mineola, NY: Dover Publications Inc.

Mackenzie, H. (2012, Oct 25). *Shamoon malware and SCADA security – what are the impacts?* Retrieved on November 26, 2019 from https://www.tofinosecurity.com/blog/shamoon-malware-and-scada-security-%E2%80%93-what-are-impacts

Roberts, J. (2012, Nov 27). *Cyber threats to energy security, as experienced by Saudi Arabia*. Retrieved on November 17, 2019 from https://blogs.platts.com/2012/11/27/virus_threats/

Sanger, D.E. (2018) *The perfect weapon: War, sabotage, and fear in the cyber age*. New York: Penguin Random House LLC.

Saudi Arabian Oil Corporation (2019) *Our corporate governance – board of directors.* Retrieved on November 14, 2019 from: https://www.saudiaramco.com/en/who-we-are/our-corporate-governance/leadership-team

Sun Tzu (1994) *The art of war.* (R. Sawyer, Trans.) Boulder CO: Westview Press.

White, S. (2019) *Lecture Notes* [PowerPoint Presentation].

Zhioua, A. (2013, July 8-11). The middle east under malware attack dissecting cyber weapons. *2013 IEEE 33rd International Conference on Distributed Computing Systems Workshops.* doi: 10.1109/ICDCSW.2013.30