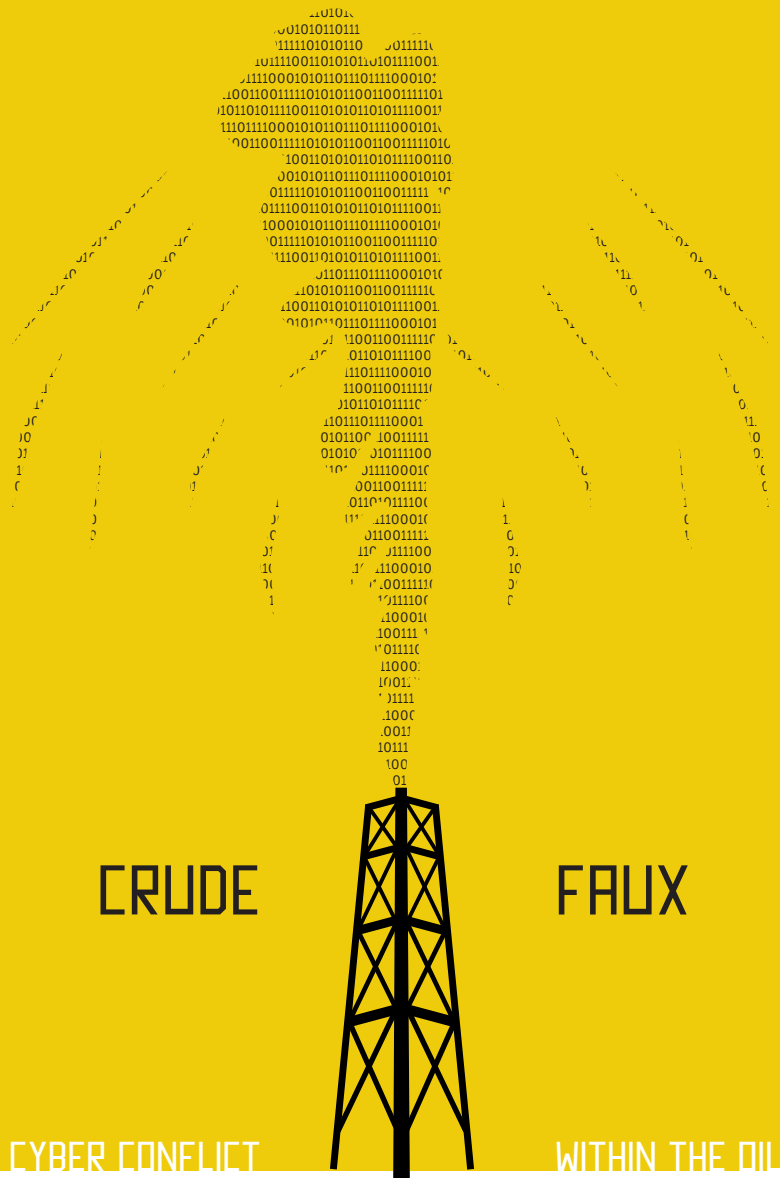


CRUDE FAUX

AN ANALYSIS OF CYBER CONFLICT WITHIN THE OIL & GAS INDUSTRIES

Authors

Jake Kambic, Kristine Aurthor, Will Ellis, Mary Horner, Tyler Jensen, Kyle Johansen, Brian Lee

Under the direction of
Dr. Samuel Liles

Abstract

The oil & gas industry is a multibillion-dollar industry that has a history of conflict. As modern technology has developed, both the corporate aspects and technical aspects of the oil & gas industry have become heavily reliant on the Cyber domain. The inherently insecure origins and evolution of computing has led that dependence to become a severe vulnerability. This report examines how these vulnerabilities have been exploited, and what that means to the future of the industry.

Purdue University

Cyber Conflict & Transational

Cyber-Crime Course

EXECUTIVE SUMMARY

The oil & gas industry is a multibillion-dollar industry that has a history of conflict. As modern technology has developed, both the corporate aspects and technical aspects of the oil & gas industry have become heavily reliant on the Cyber domain. The inherently insecure origins and evolution of computing has led that dependence to become a severe vulnerability. Recent events have brought this fact to light with a deluge of "cyber attacks" launched globally against the industry. These attacks raise specter of cyber conflict and the question of culpability. This report seeks to analyze a selection of these events, looking for patterns that would indicate one or more advanced actors. By observing the motives means and opportunities presented to actors, and looking at a cross section of these attacks over time, conclusions will be drawn as to the past, present, and future of cyber conflict within the industry.

The US Army notes in their Cyber Concept & Capabilities plan for 2016-2028 that cyber capabilities pose a unique and attractive opportunity to an inferior enemy to gain equivalence temporary equivalence with a superior enemy through the use of Cyber. This applies not only to nation states, but non-state actors as well. There are several factors compounding this issue:

- Unfettered access to the infrastructure and tools used to conduct cyber operations by anyone
- A low barrier to entry fiscally and limited experience required to achieve an outsized impact
- A high and attractive return on investment
- Plausible deniability due to issues with attribution

These facts make it highly likely that multiple foreign agencies as well as powerful corporate denizens have used and continue to make use of cyber capabilities to affect favorable outcomes.

Methods: Using OSINT techniques, information was gathered from government websites, corporate websites, news agencies, and search engine queries. This information was then synthesized and scrutinized for possible links and attribution. By looking at the surrounding geopolitical events, gains and losses as well as indirect outcomes, events can be correlated and attributed to actors which possess the means motive and opportunity to do so. The primary purpose is to analyze the event regardless of attribution. Because of the nature of open source information, biases are naturally introduced which must be acknowledged, if not accounted for.

Events: Incidents were selected based on relevance and their timeliness, along with other factors discussed in the methodology. Incidents were largely grouped into one of three categories: espionage, sabotage, and incidental/miscellaneous. While these incidents do not qualify as warfare by the Clausewitz definition, they are a form of conflict.

Cyber Espionage: There is significant evidence of protracted, insidious espionage carried out by a state actor within the cyber realm. China has likely launch hundreds of cyber attacks against the oil and gas industry since as early as 2002. With the advent of Red October, they may not be the only actors in the game. With a level of sophistication not yet observed publicly in this realm, Red October could represent an evolution to China's current techniques, or another actor entering the game. By looking at some of the technical aspects of the events, a link was established between Byzantine Candor and APT1, as well as a possible link between the Mirage Campaign and Elderwood Project.

Sabotage: The Middle East has scene perhaps the most evidence and variety of cyber conflict of all. While staying away from events which do not directly relate to the oil industry, a series of sabotage incidents using cyber as the medium are examined. It is possible that there events were salvos between nation states in an example of bidirectional conflict. If this is not the case, and incidents like Shamoon were simply the act of non-state actors, then it represents affirmation of the revelence of non-state actors in future cyber conflict. This is only logical since most of America's critical infrastructure is controlled by the private sector, and economic influence can be leveraged to gain great power.

Incidental: By taking an adversarial look at the Deepwater Horizon oil spill, an example of how a state actor could act in a violent, kinetic way against a non-state through cyber while remaining anonymous is examined through a vignette. It is determined that while the Deepwater horizon spill was not an attack, it easily could have been. This type of conflict is both deadly and catastrophic, and while it is unlikely to be used lightly, it sets the tone for possibilities going forward.

Conclusions:

Based on the observed events, the possible threat actors, and the correlation of these events, it appears that there is ongoing cyber conflict within the oil industry. The correlation of several incidents has shown coordinated attacks by an advanced foreign threat actor against multiple entities with the use of espionage. It has also suggested the possibility of more destructive attacks, and pointed out the benefits to both state actors and non-state actors within the oil industry. In some cases there has been an obvious alignment of political, strategic, operational, and tactical goals and principals to affect favorable outcomes. The culmination of these findings is that there are many threat actors who are currently engaged in, or may be engaged in, ongoing conflict which may have the potential to escalate. This should be both a primary concern and a cause for future research and analysis.

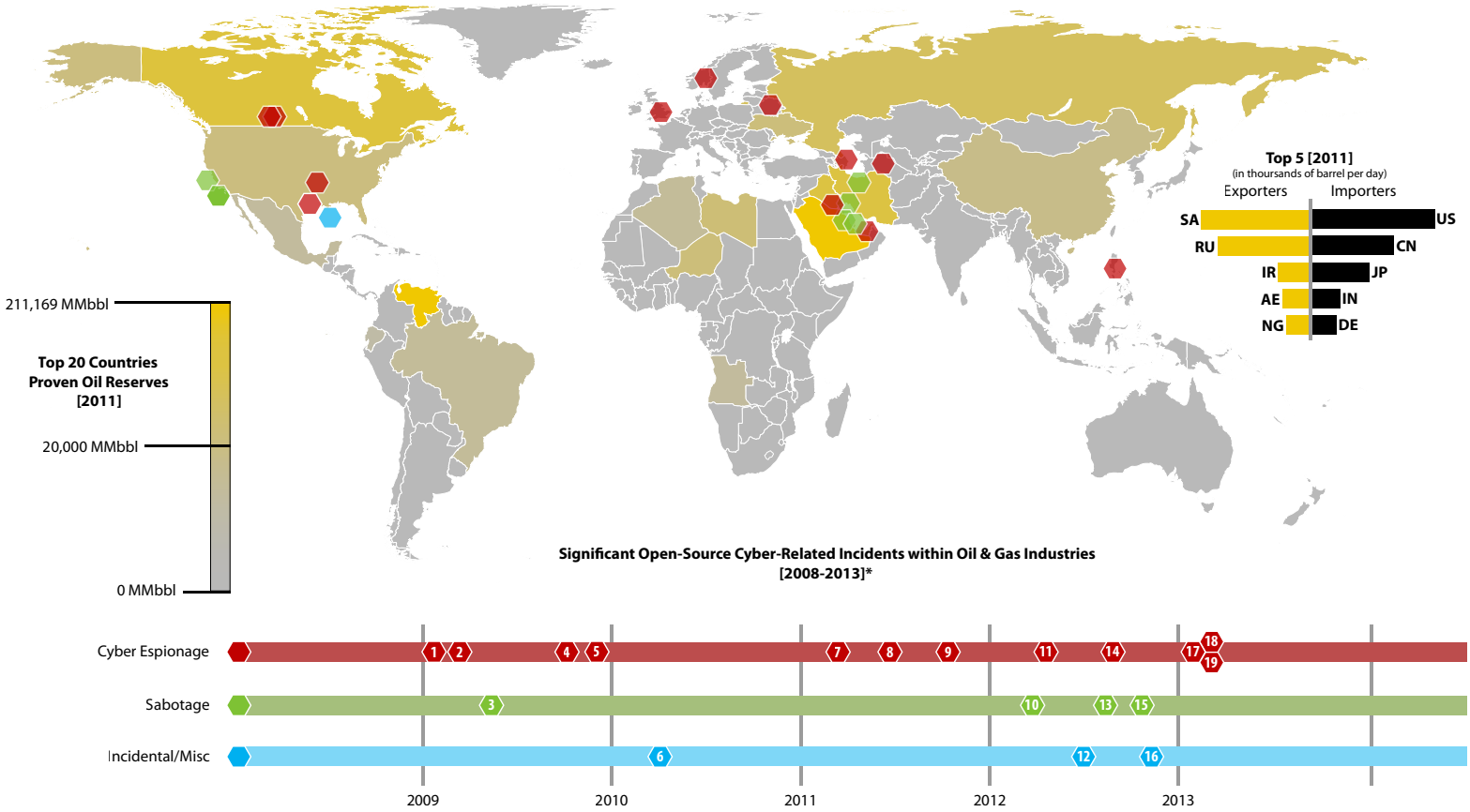
INTRODUCTION

Recent events of national significance within the oil & gas Industry have brought to light both the question of defining threat sources and that of plausibly attributing known events to a threat source. The unprecedented rise in cyber events begets the question of whether this is incidental to the continued advancement of technology, or suggests an ongoing conflict that may escalate. This report will aggregate relevant events, present criteria for outlining threat origins, and determine the likelihood that the incidents are related. It also seeks to determine whether or not any observed correlation points to a persistent aggressor or simply circumstantial coincidence. The purpose of this analysis is to provide decision-makers with a clearer idea of the current security outlook for the oil and gas industry, and pinpoint what current and future causes for concern appear to be. All events and presented options should be considered cautiously and as empirically as possible; any assumptions that are made will be explicitly stated.

TIMELINE OF EVENTS

One of the first priorities is to outline a timeline of events which have occurred and then examine what significance they may have or relationships they may share in order to scope the conversation. These events will constitute the frame for the analysis. Events were chosen after a preliminary overview of content from open sources such as established news media sites, oil & gas company websites, Google query results, government bulletins, and technical reports by security companies. From this brief overview, events within the Oil and Gas Industry which exhibited a “cyber” component were selected. These events are not meant to be all inclusive, and due to the entirely open source nature of the resources, the vantage point on the information may be biased and in many instances is likely incomplete. However even an incomplete view may contain enough information to identify significant patterns, and by acknowledging the quality concerns with the information, a more accurate and objective analysis may be performed. Below is a timeline of observed events which will be discussed in greater detail. The timeline will list the event and the apparent target of the event.

TIMELINE & DETAILS OF SAMPLED EVENTS



Significant Open-Source Cyber-Related Incidents within Oil & Gas Industries [2008-2013]*

1. Sophisticated infection and data exfiltrationin Iraq of corporate secrets suspected to be part of the Night Dragon campaign
2. Earliest known intrusion of Shady RAT in the Gas industry–sophisticated infection and data exfiltration of corporate secrets
3. A disgrunted former contractor for PER intentionally disables offshore oil rig safety controls remotely off the coast of California
4. McAfee starts monitoring the Night Dragon cyber espionage campaign against oil, energy, and petrochemical companies
5. Symantec ties back a Google hack to a campaign referred to as the Elderwood Project that targets Oil/Gas targets amongst others
6. Deepwater Horizon Oil Rig suffers catastrophic failure; Control safety Systems had been rendered inhibited
7. BG Group Plc and CHK. are alleged to be victim of sophisticated data exfiltration of corporate secrets reported by Bloomberg
8. Talisman Energy & Halliburton Co. are targeted by the comment group as part of a corporate espionage campaign
9. Sophisticated infection and data exfiltration of corporate secrets from unspecified oil & gas companies in Norway
10. Virus infects a series control systems on Kharg Island, Iran's main oil exportation station, causing them to shut down the terminals
11. Dell's Counter Threat Unit begins tracking the Mirage cyber espionage campaign—Sophisticated data exfiltration of corporate secrets
12. Anonymous hackers target oil industry giants, exposing more than 1,000 email credentials
13. Shamoon virus systematically exfiltrates corporate data and wiped hard drives of over 30,000 computers at Saudi's Aramco
14. Sophisticated infection and data exfiltration of corporate secrets from Telvent, ltd.
15. Virus infects a series control systems on Kharg Island, Iran's main oil exportation station, causing them to shut down the terminals
16. Anonymous announces their intent to attack international oil companies in "#OpFuelStrike"
17. Kaspersky announces Red October, a highly flexible cyber espionage virus which targets, amongst others, global oil & gas companies
18. Mandiant releases a document entitled APT1 which implicates China's PLA sponsored espionage, including within the Oil Industry
19. The CSM highlights a "restricted" DHS report states 23 gas pipeline companies were targeted via spear-fishing

Given this data set, a natural escalation of events appears to occur, with the frequency of incidents continuing to rise. This can partially be explained by a growing international awareness of the vulnerabilities and perils involved in internet-facing control systems of all kinds; as events occur, they garner additional attention and therefore induce additional incidents.

However, there are other interesting observations to be made from this data. Largely, the incidents of great note have occurred in either North America or the Middle East. When considering that three of the top five oil producing countries are in these regions (Saudi Arabia, the United States, and Iran), this is not surprising. Yet substantive reports of similar incidents are markedly absent in the other two of the top five oil producing countries (China and Russia), and this is noteworthy. The argument could be made that this is due to language barriers and tight control on information dissemination, but it is improbable that a significant incident would have gone entirely unnoticed by all media outlets. As the incidents themselves make apparent, human threat actors are involved, and what remains to be identified is whether there is the complexity, overarching coordination, or recurring threat source that would point to an advanced threat such as a state actor or complex non-state actor.

Before continuing with the possible attribution of events, some base discussion and criteria for the threat sources must be established. A threat source is considered to be a human-based or natural entity which possesses a capability that aligns with an unmitigated vulnerability. The threat sources which will be considered must meet the minimum requirement of having both the motive and the means to carry out the attack. Once a hypothesis consisting of these elements is established, it will be scrutinized to determine whether or not the events surrounding the incident or series of incidents align in any obvious political, strategic, operational and tactical manner. The means in this case consists of both the opportunity and the technological capability to cause the incident to occur, and the motives that will be considered are economic gain, retribution, or political agenda (to include ideology).

The US Army notes in their Cyber Concept & Capabilities plan for 2016-2028 that cyber capabilities pose a unique and attractive opportunity to an inferior, asymmetric enemy to temporarily gain equivalence with a superior enemy because of its relatively low initial cost, high return on investment, and plausible deniability due to issues with attribution. Because of this fact, it is highly likely that multiple foreign agencies as well as powerful corporate denizens have used and continue to make use of cyber capabilities to affect favorable outcomes. The rest of the report will attempt to substantiate this claim through critical analysis.

METHODS

To reach the conclusions presented in the ensuing report incidents were collected and chosen based on the inclusion of cyber either as the medium for the event, or as some component factor that played a direct or otherwise instrumental role in the outcome. After collecting a sampling of incidents into a dataset, these incidents were examined and several directly attributable features/impacts were taken into account, including:

- The victim(s) targeted
- Evidence of cyber involvement
- Economic losses
- Fatalities incurred
- Geopolitical impacts

Beyond the direct impacts, it was also necessary to consider possible indirect "ripple" effects. For example, it could be important to consider something like the prices of crude oil prior to and after a given incident. A circumstance may be such that particular companies or countries unaffected by the incident would find themselves benefiting from a ripple effect like higher crude prices. Other effects to identify include changes in the status of the involved companies throughout an incident. This could involve looking at earnings reports, the selling or buying of assets, or any legal actions the company is involved in, as well as contextual events that are significant or contentious and occur directly prior to or after an incident.

Through the investigation of these outcomes and contexts, there is the possibility of finding correlations between various incidents. These correlations may be made plain by observable patterns among the details of the events. An observed pattern may suggest a recurring actor—these patterns include tactical and methodical similarities between alleged attacks, recurring targets, entities that directly or indirectly benefitted or incurred losses as an outcome, and geographic dispersion or closeness of the events. In cases where an attack is apparent, tactical elements such as tools were scrutinized as well, as a means of attribution. For example, a tool may unintentionally exhibit cultural tendencies such as the language used, colloquialisms, idioms, religious preference, and recurring personal habits of the creator or operator. These signatures coupled with aspects of the tactical assets like exclusiveness (as in the case of a purchased domain used as a C2 point) can significantly raise the confidence level of an attribution.

Possible actors in the cyber exchange can ostensibly be identified from these correlations. If it is determined that the incident was an attack, motives of the potential actors can be considered. A key element of this that should be considered is any precedence for the attack. The history of political relationships between countries, such as any expressed hostilities or allegiances and treaties, may also prove relevant. History also tells us that most conflicts arise over the acquisition of resources. As such, the energy resources and requirements of nation-states must be analyzed. For example, is the entity being examined a major importer or exporter of oil? Is the entity capable of energy self-sufficiency? Or has the country been experiencing a major influx in energy demand? This information can then be aggregated and synthesized into a more informed view of the event.

A final major component of the analysis was the examination of whether the motives and methods align with the actor's strategic culture. This includes defining the overall strategic theories that the country adheres to and goals it desires to accomplish. As mentioned earlier, the tactics employed during the attack can be incredibly potent as an attribution mechanism—if an attack is far removed from a nation's capabilities, it is less likely that they were involved in the incident. Likewise, if the tactics are within a given nation's technical prowess and follow established patterns exhibited by that nation, it significantly improves the confidence in attribution. However, caution was taken when attributing tactics to actors, as deception is a common element in many cyber warfare strategies. Therefore, tactical similarities or dissimilari-

ties alone do not implicitly identify or rule out a given actor.

Biases

The nature of OSINT gathering poses obstacles to objective analysis. While gathering the data, it should be noted that there are source biases. All of the sources used are open source, and as such the provenance of the information cannot always be independently verified. The information itself may be legitimate, but presented in an incomplete or skewed manner. It is also likely that not all of the details of the collected incidents are available. In some cases the companies reporting the incidents, such as Symantec and MacAfee, are not legally disposed to divulge select information about their customers. Another limitation is information available about incidents that occurred in foreign countries. Due to tighter control over journalism or language barriers, other countries are likely not releasing full details from incidents that have occurred or not doing so in languages familiar to the authors. In some cases, entire events may not be released to the public, either by foreign governments or the companies themselves.

In order to address the above concerns, several methods were used. Data was gathered from established, and ideally trustworthy, sources. This includes reports from reputable news sites, company or government publications, or scholarly papers. Also, every effort was made to track down the original source of the information found in reports, or cross-examine it with other sources. Multiple sources were found wherever possible and scrutinized in order to obtain corroborating data. Of equal interest is information which was contradictory between sources. These contradictions were presented and addressed where appropriate.

Finally, despite evidence found in support of any given actor, alternate hypotheses must be considered. As with any intelligence gathering, there is the possibility of error, whether information is misreported or taken out of context, and this is especially true of OSINT. The purpose was not to select an outcome and attempt to support it but rather to find refutation as well. Information that may exculpate a particular actor was thoroughly considered. Although human error is common in cyber incidents, it is important to determine whether the error was taken advantage of by others.

CYBER ESPIONAGE

One of the most easily distinguishable patterns on the above timeline is the growing frequency of reported cyber espionage. This saga of long-term campaigns has been garnering a lot of attention, and with good reason. Some have asserted that certain campaigns have existed since the early 2000's[1], yet their existence has only recently come to light in the private sector. The damage caused by these types of breaches is difficult to estimate because it occurred over such a long time span, but in some cases terabytes of data were stolen over the period of a few months.[2] When taken in relation to the oil industry, where proprietary information like bid exploration data is the lifeblood of the organization, this can be a disastrous blow. However, while campaigns like "Night Dragon" are pointedly targeted at the oil industry, others are far more encompassing in their breadth and appear more disparate.

Establishing a baseline or pattern within this industry alone excludes a large and potentially useful amount of context. Not only were most of these cyber espionage campaigns larger in scope than simply the oil and gas industry, but some also completely excluded it. Interestingly, there are other cyber espionage campaigns not listed in the timeline (such as the infamous Flame and Mahdi viruses) that target countries with some of the largest oil reserves in the world, but the attacks themselves were not targeted at the Oil & Gas Industries.

Given the sheer number of incidents, it would seem likely that there is more than one source, yet the technical data available seems to suggest otherwise. It is clear that these incidents represent a huge danger to the profitability and competitiveness, even the future success, of victim companies; Yet these consequences carry with them some level of inherent attribution. The very nature of proprietary information means that if an entity who had acquired it were to use the information, it could identify them as having a connection to the incident, whether directly or through a third party. Also, attacks of this scale require some level of organization that manifests itself in the form of repeated patterns of behavior and resource usage that can suggest a common origin. This organization coupled with the resources and expertise necessary to process and analyze the exorbitant volume of stolen information leads to a high likelihood of state actor or organized criminal involvement.

One of the largest difficulties present in identifying the provenance and totality of these attacks is that there is no publicly available aggregation of the body of information collected on the various APT activities. Instead, Antivirus & Incident Response firms which have the best vantage point on the situation are providing separate reports in which they use their own colloquial names and terms for the attacks, the tools, and the campaigns. This creates overlap, where campaigns with different names may in fact be part of the same campaign, and the technical data that is otherwise separated across the reports could together represent a more apparent pattern. Only one report, the Mandiant APT1 report, included a brief table noting that they had compared some of the other attacks and ruled out APT1 as the culprit. Additionally, these firms are entrusted with the safeguard of their customers' information, and so often will not release the full extent of what was found, nor a definitive list of victims – adding to the obscurity. These sources also introduce their own biases which must be accounted for.

For this reason, what follows is an overview of the various reports that mention the oil and gas industry as targets, and an analysis of important technical aspects and goals of these campaigns. Through this analysis, hopefully a more complete view of the action may be obtained to see if the goals, resources, techniques, and timeframes exhibit commonality between attacks.

---

1 Mandiant, APT1 (Feb 13, 2013). Retrieved from http://www.mandiant.com/apt1

2 Ibid.

OIL/GAS INCLUSIVE OR SPECIFIC CAMPAIGNS

'Countries affect' lists only countries where oil and gas companies were compromised.

Campaign: NightDragon

Publisher: McAfee

Synopsis: The NightDragon report released by McAfee was somewhat of a seminal event in that it was the first well known release of a fairly detailed APT analysis and technical attribution. The attacks conglomerated in NightDragon were nearly all conducted against unspecified "global oil, energy, and petrochemical companies." The attacks followed a methodical series of steps:

1. using SQL-injection to obtain access to an extranet server, or using spear-phishing against "mobile worker laptops" and "compromising corporate VPN accounts" to obtain access to the company intranet
2. uploading common hash dumping tools & password cracking tools harvest Active Directory credentials to gain access to sensitive desktops & servers
3. Access sensitive documents
4. Upload RAT malware to exfiltrate sensitive data
5. Move laterally

McAfee was also able to identify much of the generic malware used, and communications techniques. They also suggested that the attackers worked between 9:00am and 5:00pm Beijing time during weekdays, and that most traffic was originating from the Shandong Province of China.

Published: Feb 10, 2011

Earliest Date: "[Attacks have been ongoing for] at least two years, and likely as many as four"

Circa 2007-2009

Purpose: Exfiltration of "competitive proprietary operations and project-financing information with regard to oil and gas field bids and operations" & collection of data from SCADA Systems

Entry Method: Social Engineering, Spear Phishing, SQL-injection

Countries with Companies Affected: U.S., Taiwan, Kazakhstan, Greece

Campaign: Elderwood

Publisher: Symantec

Synopsis: Symantec observed a group it refers to as the Elderwood gang operating a concerted campaign against a variety of industries including an undisclosed oil and gas company. Symantec also asserts that these are the same hackers who operated in the "Aurora" campaign against Google in 2009. This campaign is unique to some degree in that it used a high number of zero day exploits in Adobe Flash and Microsoft's Internet Explorer. While it appears that the attackers used spear-phishing (via email), their primary technique was the use of a "watering-hole" attack whereby they attack websites known to be frequented by the target using techniques such as SQL injection, and upload malicious files to these website. The target then visits the site and gets infected. This is interesting because the target does not have any indication that it has been compromised, but the number of overall infections goes up because of untargeted victims which also visit the site. This attack requires the attackers to find security vulnerability in the desired website after selection, requiring more technical skill than some of the other campaigns initially exhibit. Symantec believes that the exploits were packed with a Trojan and Command & Control (C2) server address using a platform that gives the group its name: "Elderwood."

Published: Sept 06, 2012

Earliest Date: December 2009

Purpose: "the wholesale gathering of intelligence and intellectual property"

Entry Method: Watering-Hole attacks, Spear Phishing

Countries with Companies Affected: Undisclosed

Campaign: ShadyRAT	**Publisher:** McAfee
Synopsis: This report released by McAfee discusses a RAT they claim to be incredibly prolific, infecting a variety of industries across multiple countries. The report itself is very sparse on any technical details or evidence, largely lacking substance. It provides a list of victims by industry and their country of origin. It also provides a detailed timeline for the attacks. Interestingly, Eugene Kaspersky heavily criticized the report for being alarmist and skewed, stating that many of the conclusions were presumptive. **Purpose:** Exfiltration of "a historically unprecedented transfer of wealth—closely guarded national secrets (including those from classified government networks), source code, bug databases, email archives, negotiation plans and exploration details for new oil and gas field auctions, document stores, legal contracts, supervisory control and data acquisition (SCADA) configurations, design schematics, and much more" **Entry Method:** Spear Phishing **Countries with Companies Affected:** U.S.	**Published:** August 02, 2011 **Earliest Date:** July 2006

Campaign: Mirage	**Publisher**: Dell SecureWorks
Synopsis: Dell SecureWorks gives a fairly good collection of technical details about the campaign they've dubbed "Mirage" for the string used to connect to the C2 server by the Remote Access Trojan, but largely they focused on studying the tool, not monitoring the APT activity. Some points of note are the use of HTRAN (a relay that Dell's Cyber Threat Unit asserts was developed by the Honker Union of China, or HUC) for relaying, and registry of a few domains to an email address (dnsjack@yahoo.com) and IP ranges in China. **Purpose:** Theft of "intellectual property and company secrets" **Entry Method:** Social Engineering, Spear Phishing, SQL-injection of web servers **Countries with Companies Affected:** Philippines, Canada	**Published:** Sep 18 2012 **Earliest Date:** April 2012

Campaign: Red October

Publisher: Kaspersky

Published: Jan 14, 2013

Earliest Date: May 2007

Synopsis: Red October is a sophisticated espionage network very much unlike other attacks which had been reported. While for the most part, the targets were diplomatic, there were several instances where Kaspersky noted that oil and gas industries had been targeted. The attack used domains registered to Russian email addresses, and IP ranges identified were serviced by largely German and Russian ISPs, however Kaspersky believes that the three "mothership" C2 servers identified are actually themselves proxies for an as yet unidentified C2 server which could then be operating nearly anywhere. A salient point is that Red October made use of exploit code that was "created by other attackers and employed during different cyber attacks. The attackers left the imported exploit code untouched, perhaps to harden the identification process." Additionally, Red October is somewhat unique amongst attacks that targeted oil and gas in that it is capable of stealing information from a variety of embedded devices such as phone and routers.

Purpose: "gather intelligence from the compromised organizations"

Entry Method: Social Engineering, Spear Phishing, SQL-injection of web servers

Countries with Companies Affected: Azerbaijan, Belarus, Turkmenistan, UAE

Campaign: APT1

Publisher: Mandiant

Published: Feb 19, 2013

Earliest Date: 2004-2006

Synopsis: The APT1 Report is perhaps the most detailed report to date. They also minced no words, directly accusing China as a state actor of engaging in Cyber Espionage. Researchers at Mandiant tracked back activities of an APT group they referred to as APT1 to the Chinese PLA Unit 61398 with relatively solid evidence. They even went so far as to report the building which they believed APT1 was operating out of, and unmask three operators – UglyGorilla, DOTA, and SuperHard – giving possible real names, online personas and other identifying information about them. APT1 operated over half a decade at least, stealing "hundreds of terabytes of data from at least 141 organizations," often conducting such operations in parallel. The attackers maintain access to a given network for nearly a year on average. The attackers operated during the 9:00am to 5:00pm Beijing Time and thy followed a fairly strict methodology of attack, similar to the one noted in the NightDragon report:

1. Initial reconnaissance
2. Initial compromise of a system, largely though spear phishing
3. Establishing a foothold in the network through Trojan dropping to a C2 server
4. Escalating privileges through credential harvesting
5. Internal reconnaissance of the network and

While Mandiant generically refers to energy companies, one of the trojaned files they note was used in the spearfishing attack bears the name "Oil-Field-Services-Analysis-And-Outlook.zip" which really ties. Mandiant notes that APT1 is also referred to as the Comment Group, a name given for the communications method used by their RATs which would set attributes in web pages as a means of C2.

Purpose: Exfiltration of "competitive proprietary operations and project-financing information with regard to oil and gas field bids and operations"

Entry Method: Spear Phishing

Countries with Companies Affected: Undisclosed

Campaign: Byzantine Candor

Publisher: Bloomberg

Synopsis: An exposé run by Bloomberg in 2012 chronicled the undertakings of a security research coalition which decided to track one of the largest Cyber Espionage groups operating out of China. Bloomberg claims that US Intelligence had been keeping tabs on the group for years, which they referred to as Byzantine Candor. In the same breath, Bloomberg notes that the group is often referred to as the "Comment Group." Bloomberg journalist Chloe Whiteaker also published a short but technical article that detailed some of the Comment Groups activities and tools. The report included an infographic that identified oil and gas victims of the comment group.

Published: July 26, 2012

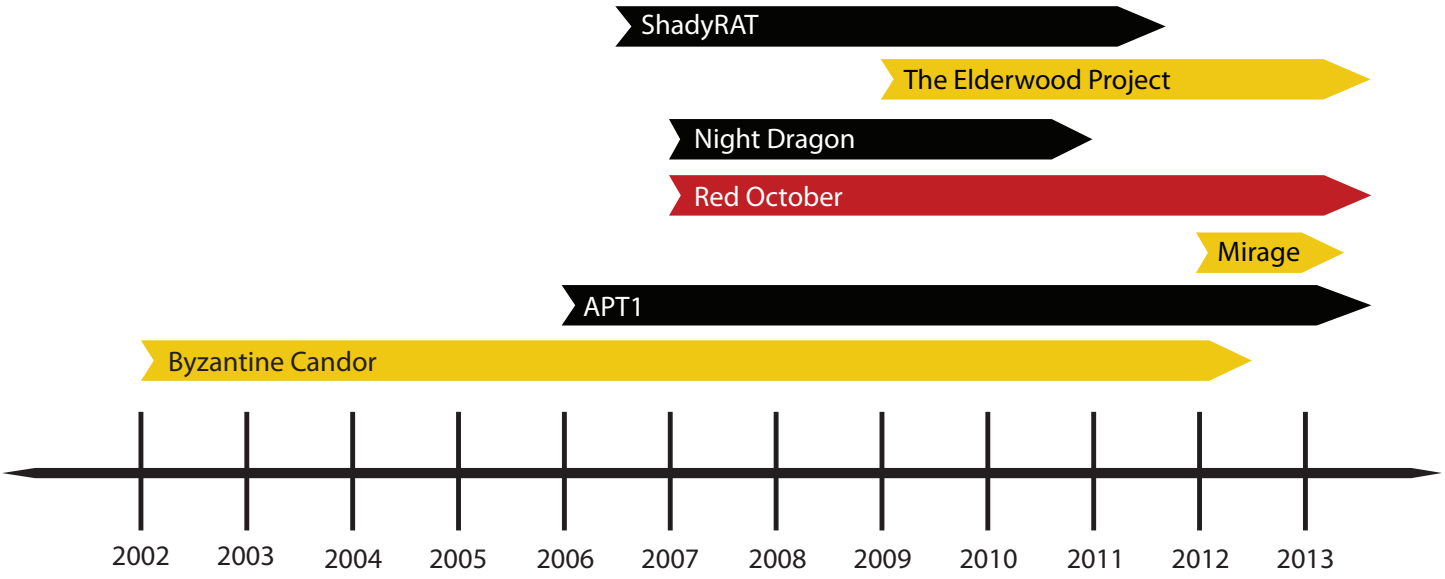
Earliest Date: 2002

Purpose: "the biggest vacuuming up of U.S. proprietary data … ever seen"

Entry Method: Social Engineering, Spear Phishing

Countries with Companies Affected: U.S., United Kingdom

REPORT BASED ATTACK TIMELINE



TECHNICAL SIMILARITIES

Between the campaigns identified above, there are a few technical similarities that arise. As was already addressed, these attacks have been selected for one common thread they share – targets within the oil and gas industry. Other between them will now be scrutinized to find any additional links. This is not intended to suggest that the same group is behind every attack, but rather identify tactical and operational similarities that would point to a unified source of training or control.

One of the most obvious similarities between all of the attacks is the motive: the large scale theft of corporate data. The methodology of data extraction is very similar between Night Dragon, Shady RAT, Elderwood, APT1, and Byzantine Candor. One note on this is that although the attacks all followed a similar methodology, this very methodology is common in the network penetration t world, and so not entirely unique. Slides from a presentation given by SANS affiliate James Shewmaker in 2008 highlight this methodology in brief: Reconnaissance, Port/Vulnerability Scan, Exploitation, and Repeat from the new vantage point. The only thing largely different is that the data exfiltration occurs after exploitation – that and the attackers were working from the outside initially, so they used social engineering to get in. With that

said the fact that the majority of these used highly targeted spear phishing and exfiltrated similar data using RATs is not to be discounted. Additionally, these attacks all appear to be operating out of either Beijing, Shanghai, and Shandong province.

The data below will show that Byzantine Candor and APT1 are one in the same – they share operators (Ugly Gorilla) and unique technical infrastructure like Fully Qualified Domain Names (FQDNs). Mandiant tied APT1 back to the PLA, and a . Mandiant even acknowledges the article written by Bloomberg in their report, and identifies the "Comment Group" as an alias

IP ADDRESSES & ORIGINS

While about half of the reports omitted IP ranges, the majority of IP address ranges mentioned came from service provided by China Unicom to one of two locales: Beijing or Shanghai. The major exception to this is Red October, which largely had IP address ranges coming from Germany and Russia. Excluding Red October, in cases where ranges did not come from Beijing or Shanghai, they were often identified as host that were compromised and used as proxies loaded with tools such as HTRAN.

Night Dragon	Elderwood	Mirage	Red October	APT1
[unspecified IP range – most C2 servers operating out of Heze City, China]		114.240.0.0/20	141.101.239.225	223.166.0.0/15
			178.63.208.49	58.246.0.0/15
				112.64.0.0/15
				139.226.0.0/15
				114.80.0.0/20
				101.80.0.0/20

Interestingly Night Dragon, which does not provide a range of IP addresses, offered instead that an individual operating out of Heze City, Shandong, China was responsible for providing the C2 servers through his company. An article published in the Wall Street Journal notes that McAfee identified this individual as "Song Zhiyue."[3]

DOMAINS

A full list of domains retrieved from the various reports can be found in the appendices. Of the domains which appeared in the reports, only matches between APT1 and Byzantine Candor were identified. The rest were inconclusive as some of the reports did not include FQDNs and others which did include them did not provide a full list. Additionally, a large portion of the attacks made use of Dynamic DNS services, where the parent domain is not inherently malicious. But subdomains may be used by service subscribers for their own purposes without policing.

Registered domains common between APT1 & Byzantine Candor
*.hugesoft.org
www.arrowservice.net
www.blackcake.net
www.dnsweb.org
www.globalowa.com
www.purpledailt.com
www.worthhummer.net
www1.earthsolution.org

3 Hodge, N. & Entous, A. (Feb 10, 2011). Oil Firms Hit by Hackers From China, Report Says. Retrieved From http://online.wsj.com/article/SB10001424052748703716904576134661111518864.html

With that said, there is another somewhat tenuous connection between two of the campaigns: Mirage and Elderwood. Night Dragon is not the only instance where an individual in China is charged with providing infrastructure to the attackers via their business – HB Gary authored a report in the wake of Operation Aurora which implicated a business called Bentium operating 3322.org out of Changzhou and a man named Peng Yong as providing dynamic DNS services to the attackers.[4] Operation Aurora was tied to Elderwood in Symantec's Elderwood Project report and elsewhere. Dell Secureworks which authored the Mirage Report also authored a piece known as the Sin Digoo Affair.[5] The connecting factor between the Sin Digoo affair and Mirage was that an operator reused several email addresses (jeno_1980@hotmail.com & king_public@hotmail.com) and infrastructure between them. The C2 servers used a Dynamic DNS service operated by 3322.org. The Sin Digoo Affair also ties these back to Gh0stNet via 3322.org and the RSA breach based on the reuse of IP address blocks belonging to the "China Beijing Province Network (AS4808)." Peng Yong also owns other domains tied back to malicious use both in Aurora and elsewhere. According to Steve Ragan of the Tech Herald, Peng Yong is possibly the author of the CRC function used in some of the Aurora malware.[6]

It is entirely possible that 3322.org was providing services to multiple separate APT groups, it is after all a fairly successfully Dynamic DNS service which has been documented in other malware cases. However, Peng's level of involvement in the Aurora campaign should be scrutinized. Interestingly the Sin Digoo report also attempts to identify the jeno_1980 account which had the alias "Tawnya Grilith" attached to it. In the process of their investigation, they tied back the account to an operator going by the screen name "xxgchappy." They also found a piece of malware ostensibly written by xxgc happy appearing to date back to March of 2002. This is potentially significant because it is the time frame around which the leaked US embassy cable had noted possible PLA cyber espionage activity. Malware used by this actor, as well as appearing in Mirage and Gh0stNet, was discovered in 2011 and 2012 to have infected government ministries in Vietnam, Brunei, and Myanmar. Additionally there are a few infected victims in Europe and the Middle East belonging to "government ministries in different countries, an embassy, a nuclear safety agency, and other business-related groups."[7] This is of interest in part because Red October also targeted government ministries and embassies.

However, in order to more fully analyze any connections between the domains that were listed in each of the reports, the whois and ARIN records could be examined. The contact information could then be cross-referenced to find similarities. Unfortunately, many of the domains had their contact information scrubbed or have since changed hands in the wake of the reports being released, so an analysis at this point would be erroneous and incomplete at best.

A final note on domains is that many of the reports did look for registrant information – in the case of APT1 for instance, many registrants blatantly put China as their place of origin, or poorly masked this fact by misspelling the places they chose or including a Shanghai phone number. In the case of Red October however, all registrations with the exception of one were done with ".ru" email addresses, and addresses were not reused as had been the case in other instances. This signals a much more concerted effort to remain anonymous, and a level of professionalism not seen in the other attacks.

4 HB Gary. (Feb 10, 2010). Operation Aurora. Retrieved From http://hbgary.com/hbgary-threat-report-operation-aurora

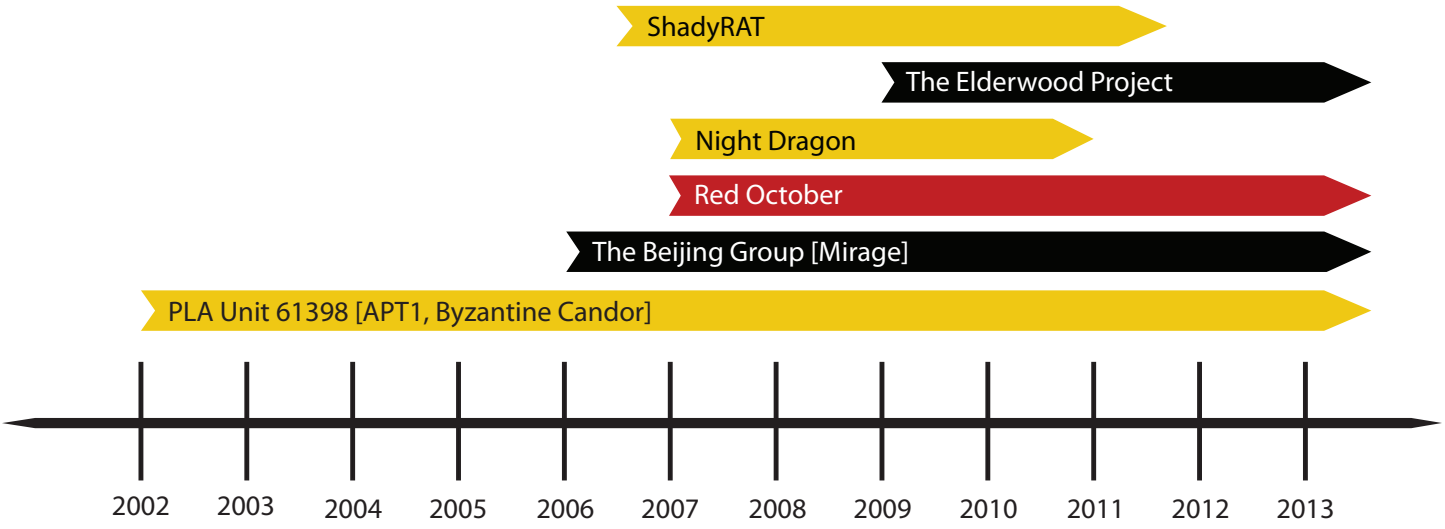
5 Stewart, J. (Feb 29, 2012). The Sin Digoo Affair. Retrieved from http://www.secureworks.com/cyber-threat-intelligence/threats/sindigoo/

6 Ragan, S. (Jan 27, 2010). Was Operation Aurora really just a conventional attack? Retrieved from http://www.thetechherald.com/articles/Was-Operation-Aurora-really-just-a-conventional-attack/9124/

7 Stewart, J. (Feb 29, 2012). The Sin Digoo Affair. Retrieved from http://www.secureworks.com/cyber-threat-intelligence/threats/sindigoo/

REVISED ATTACK TIMELINE

Considering the information which was discussed and presented, below is a revised attack timeline, consolidating individual campaigns into the likely perpetrator of the attack and extending as necessary.



EVENTS THAT CORRELATE

Using the technical data and behavioral analysis above, individual incidents of reported hacking in news media can be connected to campaigns. Below are several incidents that demonstrate strong correlation to the information discussed above.

Norway, November 2011

Norway had the most prolific series of cyber-attacks in the country's history in November 2011.[8] As reported by Norway's National Security Agency (NSM), more than 10 firms were targeted by an advanced persistent threat using spear-fishing attacks, many of which were in the oil industry.[9] The attacks may have been ongoing for over a year. The companies were unaware of the attacks until concerned employees reported receiving suspicious emails.

No specific information was released on the tools or malware that were used to conduct these attacks; however NSM noted that a virus was used in conjunction with tailored spear-fishing attacks making use of trojan attachments.[10] It appeared that the purpose of the attacks was large-scale data exfiltration. As was the case in Night Dragon, the NSM bulletin suggests that the attacks varied slightly each time so as to avoid AV detection. An article by Defense News quotes NSM as stating that "the attacks have, on several occasions, come when the companies have been involved in large-scale contract negotiations."[11] This could suggest that the attackers were privy to the negotiations. Interestingly, in 2010 Norway's Statoil was engaged in negotiations with China Oilfield Services, Ltd. (COSL). According to the Wall Street Journal, COSL is the "oil-field services and rig-construction unit of state-controlled China National Offshore Oil Corp., the country's

8 BBC News. (2011, November 18). Hackers attack norway's oil, gas, and defence businesses. *BBC News Technology.* Retrieved from http://www.bbc.co.uk/news/technology-15790082

9 France-Presse, A. (2011, November 18). Norwegian defense firms hacked, intel reports. *Defense News.* Retrieved from http://www.defensenews.com/article/20111118/DEFSECT04/111180309/Norwegian-Defense-Firms-Hacked-Intel-Reports

10 NSM (2011) Samme aktør bak flere datainnbrudd . Retrieved From https://www.nsm.stat.no/Aktuelt/Nytt-fra-NSM/Samme-aktor-bak-flere-datainnbrudd/

11 France-Presse, A. (2011, November 18). Norwegian defense firms hacked, intel reports. *Defense News.* Retrieved from http://www.defensenews.com/article/20111118/DEFSECT04/111180309/Norwegian-Defense-Firms-Hacked-Intel-Reports

largest offshore oil and gas company by output."[12]

The goal of the attacks appeared to be the collection of confidential information, such as user names, passwords, industrial drawings, and other proprietary documents.[13] This would seem to be consistent with the types of information sought in both Night Dragon and APT1. The timeframe of the attack aligns with the event timeline listed in the APT1 report, and within the report there is an event appearing in Norway. This is then a convergence of time and objectives across these operations which complement the tactical similarities involving the use of social engineering, persistent backdoors, and large scale data exfiltration.

Telvent, September 2012

In September 2012 Canadian energy company Telvent was infiltrated. Telvent is responsible for supplying control programs and systems for over half of the oil and gas pipelines in North and Latin America.[14] The attackers installed malware which they used to steal project files related to Telvent's OASyS SCADA product. According to security blogger Brian Krebbs, OASyS is "a product that helps energy firms mesh older IT assets with more advanced 'smart grid' technologies."[15]

The infiltration follows the same methodical approach exhibited in the Night Dragon and Norwegian intrusions. Not only was the malware difficult to detect, but it was planted using spear-phishing methods that targeted mid to high level executives[16] [17].

Perhaps the most convincing piece of evidence as to the origins of the attack is what appears to be a notification released by Telvent which identified malicious files and domains used for Command and Control (C2). The filenames "fxsst.dll" and "ntshrui.dll" which appear in the Telvent notification also appear in the APT1 report, along with the domains "hugesoft.org" and "bigish.net" which are noted as mainstays of APT1 by Mandiant. Several security firms at the time also reported the belief that the attack had been perpetrated by the "comment group" an alias in the Mandiant Report for APT1. In fact, Mandiant actually mentioned the Telvent attack in their report under a section entitled "APT1 in the News."

The reason the Telvent attack is so important is that it represents the possibility for departure from simply data exfiltration. Although available information indicates that the goal of the attack was stealing software, the software could just have easily been modified and replaced. Attacking a prolific energy ICS company like Telvent means that a trojan could be planted in the software, being unintentionally distributed to Telvent's customers and offering the perpetrator an avenue for more insidious attacks.

---

12 Simon Hall (2013, December 13). China, Norway Strike Oil Deal Despite Tensions. *Wall Street* Journal. Retrieved from http://online.wsj.com/article/SB10001424052748703727804576016841533225226.html

13 Ibid.

14 Vijayan, J. (2012, September 26). Energy giant confirms breach of customer project files. *Computerworld.* Retrieved from http://www.computerworld.com/s/article/9231748/Energy_giant_confirms_breach_of_customer_project_files

15 Krebs, B. (2012, September 26). Chinese hackers blamed for intrusion at energy industry giant telvent. Retrieved from http://krebsonsecurity.com/2012/09/chinese-hackers-blamed-for-intrusion-at-energy-industry-giant-telvent/#more-16936

16 Vijayan, J. (2012, September 21). Cyber espionage campaign targets enery companies. *Computerworld.* Retrieved from http://www.computerworld.com/s/article/9231596/Cyber_espionage_campaign_targets_energy_companies

17 Ibid.

ATTRIBUTION

CHINA

Perhaps the most readily apparent attribution is to China as a state actor – the APT1 report makes a convincing argument for this which offers a lot of very well constructed circumstantial evidence. Night Dragon highlights the use of a RAT known as zwSheel which was used both as a to perform C2 and to create custom trojans. Interestingly, upon launch zwShell displays an error dialog with a hidden text field and the program will not function unless the password 'zw.china' is entered into this hidden text field. The ranges of consecutive IP addresses used were large enough that it is likely that the Chinese government had to be involved in some capacity.

China certainly possesses the motive to commit the attacks – according to the Washington Times, China is already surpassing the United States as the number one oil importer from the Middle East[18], and poised to become the number one oil importer globally.

Increasing Demand

Chinese demand for oil has grown dramatically as its economy continues to expand. Since the mid-1990s, China has been a net importer of oil.[19] The continuous growth of the Chinese economy has resulted in vast increases in the need for fuel and petro products. China has doubled its oil consumption in the last 10 years and become the second largest consumer of oil in the world behind the U.S.[20] Like the U.S., China is now dependent on its oil imports to feed its thriving economy. It is estimated that China's import dependency could rise to over 50% by 2020.[1]

China's oil refineries are not capable of handling the current demand the economy is placing on them. There is evidence that the refineries used for fuel are at a competitive disadvantage when compared to other countries. To complicate matters, many Chinese oil refineries are also oriented to the making of diesel and not gasoline, which is in increasing demand[1].

This means China is in great need of more sources of oil and more efficient refineries. The development of improved refining and mining equipment takes years and can cost millions of dollars. Exploration costs for finding new oil reserves have almost tripled in the past decade.[21] They could save billions of dollars and shave years of research off by acquiring technology from petrochemical corporations that are already heavily invested in this continuing process. It also means that China would be able to compete in the global market place much sooner and more competitively than if they waited to develop the technology on their own. This establishes that there are significant reasons for China to act on behalf of its own oil industry and use its state resources to conduct cyber-attacks against corporate entities worldwide.

---

18 Hill, P. (March 14, 2013). China poised to top U.S. as oil buyer; increased car sales spur jump. Retrieved from http://www.washingtontimes.com/news/2013/mar/14/china-poised-to-top-us-as-top-oil-buyer/?page=all

19 Skeer, J. (2007). China on the move: Oil price explosion?. Energy policy, 35(1), 678-691. http://discover.lib.purdue.edu:3210/purdue?ctx_ver=Z39.88-2004&ctx_enc=info%3Aofi%2Fenc%3AUTF-8&ctx_tim=2013-03-09T15%3A59%3A35IST&url_ver=Z39.88-2004&url_ctx_fmt=infofi%2Ffmt%3Akev%3Amtx%3Actx&rfr_id=info%3Asid%2Fprimo.exlibrisgroup.com%3Aprimo3-Article-wos&rft_val_fmt=info%3Aofi%2Ffmt%3Akev%3Amtx%3A&rft.genre=article&rft.atitle=China%20on%20the%20

20 Index Mundi, (2012). Country comparison > Oil – consumption > Top 10. Retrieved from http://www.indexmundi.com/g/r.aspx?v=91&t=10

21 Johnson, C., (2010). Oil exploration costs rocket as risks rise. Retrieved from http://www.reuters.com/article/2010/02/11/us-oil-exploration-risk-analysis-idUSTRE61A28X20100211

China's Oil Production in Thousands of Barrels per Day[22]

As seen in the chart above, China experienced a significant increase in oil production during 2009. This spike in production could be due to information that China gained from US firms through cyber espionage actions, such as Night Dragon. The Night Dragon attacks were believed to have begun circa 2007. According to Kirk, information taken during these attacks includes market intelligence reports and information on operational production systems.[23] Similarly, the Mandiant report shows that the APT1 group has monitored Mandiant's energy industry customers from approximately the beginning of 2009 to 2012.[24] During these attacks, APT1 would export terabytes of data from the victims to China. In tandem with these revelations, China's also aggressively pursued oil supply contracts during 2009.[25] During this time major Chinese state oil companies acquired holdings in 18 different countries. China is determined to take on oil and gas infrastructure development and to acquire oil industry assets.[26]

Although there is evidence that China has been conducting cyber espionage activities against oil industry targets as far back as 2007, there is only trivial growth until 2009. This could be a result of the time and recourse commitment required to process the data that was acquired. As mentioned, both the Night Dragon and APT1 attacks stole an enormous amount of data from English speaking companies. It is necessary for English-fluent operators to sift through this data and extract actionable information to report. This information would also need to be provided to experts in the field who could recognize the its vale, and that process would have to be done discreetly so as not to arouse suspicions. This would take time. The Mandiant report comments on the fact that there are limited English-fluent operators directly involved in the technical end of APT1, which would significantly hinder progress.[27] Considering these factors and the timeframe for growth presented above, it is conceivable that the information and strategy for its use would not be available until 2009. At this point, China could act to increase the output of the holdings that they currently owned. Also, the information gained from market intelligence reports and possibly exploration reports could guide the state companies in deciding which new holdings to purchase during this time period. The new holdings would allow for increased output overall.

China's Investments

China's fervor for oil acquisition has not been limited to aggressive increases in holdings and contracts. These activities are likely only one piece of a global strategy to secure China's future oil requirements, including reserves that may not be productive today or in the immediate future. This overarching strategy has apparently led to a pattern of quiet investment, which may be a direct cause for concern in America. An article appearing in the Associated Press discusses these Chinese investments in Venezuela, the country with the largest proven oil reserves as of 2011, and throughout the Caribbean and South America. The article notes that "when Venezuela seized billions of dollars in assets from Exxon Mo-

22 U.S. Energy Information Administration. (2013, February 12). *International Energy Statistics* [Data file]. Retrieved from http://www.eia.gov/cfapps/ipdbproject/iedindex3.cfm?tid=5&pid=53&aid=1&cid=CH,&syid=2006&eyid=2012&unit=TBPD

23 Kirk, J. (2011, February 10). 'Night dragon' attacks from china strike energy companies. Retrieved from http://www.networkworld.com/news/2011/021011-night-dragon-attacks-from-china.html

24 Mandiant. (2013, February 18). APT1: Exposing one of China's cyber espionage units. Retrieved from http://intelreport.mandiant.com/Mandiant_APT1_Report.pdf

25 Hayward, D.L.L. (2009, June 18). China's oil supply dependence. *Journal of Energy Security.* Retrieved from: http://www.ensec.org/index.php?option=com_content&view=article&id=197:chinas-oil-supply-dependence&catid=96:content&Itemid=345

26 Ibid.

27 Mandiant. (2013, February 18). APT1: Exposing one of China's cyber espionage units. Retrieved from http://intelreport.mandiant.com/Mandiant_APT1_Report.pdf

bil and other foreign companies, Chinese state banks and investors didn't blink. Over the past five years they have loaned Venezuela more than $35 billion." They have similarly provided aid to countries like Ecuador, another country within the top 20 of proven oil reserves. In some cases it appears that the Chinese are making loans that the countries will likely be incapable of repaying, placing them squarely within China's control. Many of the deals included "repayment in oil and natural gas" and billions of dollars have been loaned directly to energy companies in Russia and Turkmenistan, both of which have been targeted in cyber espionage campaigns and are in the top 5 for proven natural gas reserves.

Although the IEA has predicted that America is moving towards energy independence and is poised to become the number one oil exporter by 2017, the loans are breeding closeness with and reliance on China by countries in close proximity to the US. This could allow for the Chinese to weaken American influence in the region and create agitation against the US or between other countries within the region in order to distract the US from its goals in other areas strategic to the Chinese. These deals also place China in the supply chain for borrowers' projects where China has insisted on Chinese companies being involved as a stipulation of the loan. These loans have not required any economic reforms to accompany them, meaning that countries which could not secure a loan from the IMF due to poor financial decisions may continue to flounder in spite of aid, perhaps even more so because of it. In the worst case scenario, these countries become unstable. While this may cause issues to the Chinese in some logistical capacities, it would also serve to divert some of America's attention, making the situation a palatable outcome for China.

OTHER ACTORS

An analysis of these events would be remiss without exploring any other possible attribution. Though unlikely, it is possible that there were other actors involved. As pointed out by Eugene Kaspersky in his criticism of the Shady RAT report, some of the tools and techniques are generic enough to not lend themselves to attribution to a particular entity. Even the ones that are of Chinese origin do not of themselves implicate the Chinese government, only an actor familiar with how the tool works or minimally trained in Mandarin. A large portion of these tools were freely available on underground Chinese hacking sites. Chinese hacking collectives or corporations may have been independently involved. However, due to the suspicions voiced in the leaked diplomatic cables suggesting PLA involvement[28] and Mandiant's research on the topic indicating the same[29], it is highly unlikely that the Chinese government was not involved whatsoever. These sources, and the timeframe in which the attacks occurred -- between roughly 9am and 5pm consistently over a protracted period of time[3031] -- is indicative of a formalization of the activity. This is further evidenced by the resources required to carry out the attack and the Chinese government's grasps on censorship of their citizens through technical controls. Terabytes of data infiltrating the country is unlikely to have been missed, particularly over the course of a decade of activity.

If China had been involved in any capacity in cyber espionage attacks and this had been discovered by another entity, said entity might have leveraged this knowledge to collude with them either through coercion, cooperation, or clandestinely without the Chinese government knowing. Though this may seem farfetched, a report released by a Luxemburg security firm details how, in the wake of Mandiant's APT1 report, they decided to engage in an intelligence gathering operation on the APT groups operating out of China. By scanning Chinese IP ranges for C2 servers known to be used in the APT1 attacks and exploiting weaknesses in the attackers' C2 infrastructure, they were able to access, monitor, and control the APT infrastructure without the adversary's knowledge. Bloomberg also hinted at the possibility of American security firms acting in a similar way when they "exploit[ed] a hole in the hackers' security … logging the intruders' every move as they crept into networks..." Knowing that the Chinese were actively engaged in such operations and likely turning a blind eye to any infiltration of data, another actor operating through China and attempting to incriminate China could have engaged in cyber espionage as well. This is truly a stretch of the imagination, and there is no evidence whatsoever to support this theory. The most likely case for any attribution involves the Chinese government in some capacity.

---

28 Glanz, J. & Markoff, J. (Dec 4 2010). Vast Hacking by a China Fearful of the Web. Retrieved from http://www.nytimes.com/2010/12/05/world/asia/05wikileaks-china.html?pagewanted=all&_r=0

29 Mandiant. (Feb, 2013). APT1: Exposing One of China's Cyber Espionage Units. Retrieved from http://www.mandiant.com/APT1

30 Ibid.

31 McAfee® Foundstone® Professional Services and McAfee Labs™. (Feb 10, 2011). Global Energy Cyberattacks: "Night Dragon". Retrieved from http://www.mcafee.com/us/resources/white-papers/wp-global-energy-cyberattacks-night-dragon.pdf

SIGNIFICANCE GOING FORWARD

The most important takeaway from these incidents is the significance they hold to the future of the Oil & Gas industry. Inexorably, Oil and Gas is intertwined with the Cyber domain, and will only continue to become more so as the time progresses. The increased reliance on technology means that more and more data and control will be accessible to the attackers in the future. A large contingent of the attacks relied on social engineering and spear phishing as a point of entry, though there is a shift toward "watering hole" attacks. This is significant because even as technical controls get better, unwitting employees and their behavior will continue to be a focal point in targeted attacks.

Automation via SCADA/ICS has been an integral part of the Oil industry's past and will be even more so in the future. Attacks like the Telvent attack herald an insidious turn of events for SCADA within Oil & Gas. The attackers seemed intent on stealing SCADA software, but it is conceivable that they could have taken such an opportunity to embed their own code within it, providing a capability to manipulate large swaths of North American pipeline at will. This is not meant to be alarmist, but rather considers the next evolution of attack. Leveraging malicious SCADA software to achieve a kinetic outcome is not the baseline going forward, but it is well within the realm of possibility. The nature of a capability like this means that it can only be leveraged to catastrophic effect once, so the possibility of an entity using it outside of sustained or ardent conflict is low. However using this on a micro-scale, and degrading service or quality of service through manipulation of malicious software on the PLCs or HMIs could be more viable in a peacetime setting, and less noticeable. This type of activity could be used at the height of negotiations or disputes to put an adversary in a compromising position, or simply distract them.

The Cyber-warfare doctrine of large nation-states like China and Russia that have a huge stake in the Oil & Gas Industries is one of perpetual conflict. Timothy Thomas discusses this in his books Recasting the Red Star and The Dragon's Quantum Leap. The idea of an "active defense" and keeping potential competitors "off balance" is the posture going forward. The concept of peace being a time without conflict is rapidly disappearing. As globalization has become the status quo and global economies become ever more entangled, threat of a large-scale kinetic confrontation between top tier economic powerhouses is nearly strategically unviable. Instead, both state and non-state actors will use constant conflict in the Cyber realm as a method for accruing resources and exercising control. While cyber conflict often brings to mind the idea of SCADA initiated pipeline explosions, the theft of intellectual property and business communications is far more likely to continue. This type of low intensity conflict is cost-effective and politically sustainable in an environment where direct attribution is at times difficult. The idea of a constant or long term "ally" or "strategic partner" is no longer valid – coordination will be largely issue specific, and only to the extent required to achieve an end. While coordinating on one topic nations will be in conflict on another. This is not in any way a revolutionary or new idea; however it is becoming more and more relevant to salient industries operating within their own nation state and abroad as they become far more accessible and targetable in this type of conflict.

Non-state actors will play a huge role in future cyber conflict within the oil and gas industry. The Norway attack which coincided with a meeting by a state-backed Oil & Gas company may suggest that they already are playing a role. Certainly Antivirus & Incident Response companies are playing a role as non-state actors by releasing these reports. But aside from cooperation with Sate actors, non-state actors may operate independently against other non-state actors in pursuit of competitive advantage or sabotage. Hacker collectives like anonymous could have an out-sized impact if more highly organized, and the attacks they have already carried out could become more severe – instead of simply releasing email addresses, they could release bid data, or attempt something more destructive akin to a Shamoon type attack.

The release of reports on APT is in a way its own form of cyber conflict; the rhetoric of these reports is an information influence operation, both targeted at potential customers and at adversaries. These reports also allow adversaries to see how they were detected and correct mistakes going forward. It is likely that future attacks will lack the types of unprofessional mistakes made during these campaigns. The embedding of personal signatures (a la Ugly Gorilla) or the use of passwords like "zw.china" will diminish significantly. If an attacker wished to be more anonymous, it would start to transition to open-source and generic tools exclusively – tools which are common enough that they do not provide significant attribution. Tools like the Metasploit framework provide a high degree of extensibility without offering a

significant amount in the way of attribution by tool choice. If not a transition like this, then using tools stolen from other attackers or written in other languages would complicate attribution. The move within the Information Technology world toward more forensically resistant technologies such as SSDs and Cloud Service infrastructures which make attribution and legal jurisdiction much more convoluted will continue to be a catalyst for future attacks alongside services already in use like Dynamic DNS.

These cyber espionage attacks are likely the newly established baseline for future cyber conflict within the Oil & Gas Industry. Attacks of this nature and magnitude will continue to originate from places which do not have laws against it or are complicit, including China which has a need to secure oil dominance in the future. However, increasing international pressure will necessitate more covert action, with attackers dispersing their operators or proxies throughout large geographic areas. Non-state actors will likely present APT threats in the future, including State-backed and independent competitors.

SABOTAGE

MIDDLE EAST, 2012

Another series of events may be connected as well, and while they bear no immediately apparent relationship, closer inspection is suggestive of the possibility of another underlying and ongoing conflict. To understand the context of the exchange, a non-oil-related cyber event must be briefly discussed. A relatively unprecedented cyber-attack came to light in 2010 when the Stuxnet virus hit the uranium enrichment centrifuges in Iran. Iran believes the attack was conducted by Israel or the United States. This attack had targeted the information networks of offshore platforms; however they reported that they were able to defend against the attack.[32] Iran may have thought it was Israel because they had threatened to take military action if the sanctions on Tehran's banking and oil sectors did not stop Iran from continuing their nuclear program. The attacks targeted Iran's infrastructure and communications companies, which slowed the Internet in Iran. Israel and the United States have denied being a part of this attack.

Then In April of 2012, Iran was again the target of a cyber-attack. The Islamic republic reported that a computer virus was detected inside the control systems of Kharg Island, which controls Iran's crude oil exports.[33] This virus began to attack several of the main Persian Gulf oil terminals in Iran, which forced the Iranian officials to disconnect them from the Internet to avoid spreading the virus.[34] This virus, known as Wiper, successfully erased information from hard disks at the Oil Ministry's headquarters in Tehran.[35] The headquarters had apparently been the initial target of the virus. Oil Ministry officials reported that the international selling division had not been infected, but it many security vulnerabilities were exposed. Iran is one of the world's largest oil producers and an attack could affect the market, and raise oil prices globally.[36]

As with the Stuxnet worm, Iran blamed Israel and the United States for the spread of Wiper. Iranian officials believe they were targeted because of their growing nuclear program.[37] Other affected organizations include the National Iranian Oil Processing and Distribution Company, National Iranian Gas Company, Iranian Offshore Oil Company, Pars Oil and Gas, and other companies controlled by the National Iranian Oil Company.[38] The destruction of this data doesn't provide much in the way of direct monetary gain for any criminal elements. The real advantage gained by unleashing Wiper is to put pressure on Iran by causing economic loss and reminding them that they are vulnerable. The president of the Tehran World Trade Center, Mohammad Reza Sabzalipour, believes the cyber-attack was indeed a direct message. The aim was to increase pressure so that Iran will compromise in the upcoming nuclear talks on May 23, 2012. He later states, "We are in a bloodless war. If the talks fail, Iran can expect much more of this[39]".

---

32 Erdbrink, T., (2012, April 23). Facing Cyberattack, Iranian Officials Disconnect Some Oil Terminals From Internet. *The New York Times.* Retrieved from http://www.nytimes.com/2012/04/24/world/middleeast/iranian-oil-sites-go-offline-amid-cyberattack.html?_r=0

33 Reuters., (2012, October 08). Cyber attackers target Iranian oil platforms: official. *Reuters.* Retrieved from http://www.reuters.com/article/2012/10/08/us-iran-cyber-idUSBRE8970B820121008

34 Ibid

35 Erdbrink, T., (2012, April 23). Facing Cyberattack, Iranian Officials Disconnect Some Oil Terminals From Internet. *The New York Times.* Retrieved from http://www.nytimes.com/2012/04/24/world/middleeast/iranian-oil-sites-go-offline-amid-cyberattack.html?_r=0

36 Ibid

37 Ibid

38 Ibid

39 Ibid

An oil embargo in concert with other economic sanctions by the United States and EU was announced in late 2011 in an effort to discourage any further Iranian nuclear activity. In March of 2012, the Obama administration announced that the market could withstand the embargo of Iranian oil, and raised US-Iran tensions over the issue[40]. Saudi Arabia had also indicated that it would boost oil exports to the US and abroad to compensate for the void that would be left by the sanctions on Iran[41]. As the fifth largest oil producer in the world, the Iranian oil industry accounts for about 20 percent of Iran's GDP[42]. Both the embargo and the virus represent serious and direct concerns for the Iranian government.

Then in August of 2012, only four months after the embargo, a virus named Shamoon struck Saudi Arabian oil giant Aramco.[43] The virus was triggered on a Muslim holiday when most of the company's employees were absent from work. Shamoon was designed to replace data on hard drives with a picture of a burning American flag and report the address of the computer back to a separate computer inside the company network.[44] This is potentially significant because Aramco is the world's largest producer of oil, and was originally a joint effort with the United States (Arabian American Oil Company).[45,46] Additionally, Shamoon contained a function called "Wiper" which was responsible for the deleting of files. The name "Wiper" and the shared functionality of the two are somewhat suggestive. Interestingly, a previously unheard of "hacktivist" group identifying themselves as "The Cutting Sword of Justice" took credit for the attack and not a nation state. They claim the virus has given them access to documents on Aramco's computers, but none have been published yet.[47] The attack was believed to have been assisted by an insider at the company. Another note of significance about Shamoon is that the text "Arabian Gulf" was found in the code which is pertinent because Iran has zealously guarded the title of the region as the "Persian Gulf.[48]"

Although Wiper and Shamoon share a few common characteristics, they are significantly different. Both viruses have been analyzed by Kaspersky Labs who has concluded that although Shamoon contains a wiper function that is designed to overwrite data, it is not as well-designed as Wiper and not near as efficient.[49] The care that was taken by whoever made Wiper to insure it did as much damage as possible in the shortest amount of time is what differentiates it from Shamoon's wiping feature. Since wiping a disk with hundreds of gigabytes of storage can take an extremely long time, Wiper was designed to target files with certain extensions or in certain folders to do as much irreparable damage as fast as possible. Kaspersky claims that Shamoon was merely a copycat virus that was "the work of script kiddies inspired by the story."[50] They also claim that Shamoon was probably the work of a non-state group and that Wiper was most likely

40 Mathews, C., (2012 Mar. 30). Obama moves forward with Iran sanctions despite oil price spike. Retrieved from http://blogs.wsj.com/corruption-currents/2012/03/30/obama-moves-forward-with-iran-sanctions-despite-oil-price-spike/

41 Flintoff, C., (2012). Sanctions may squeeze Iran…and raise oil prices. NPR. Retrieved from http://www.npr.org/2012/06/30/155993909/sanctions-may-squeeze-iran-and-raise-oil-prices

42 Katzman, K., (2012 Mar. 28). Iran sanctions. Congressional Research Service Report for Congress. Retrieved from http://fpc.state.gov/documents/organization/187388.pdf

43 Perlroth, N., (2012, Oct. 23). In cyberattack on Saudi firm, U.S. sees Iran firing back. The New York Times. Retrieved from http://www.nytimes.com/2012/10/24/business/global/cyberattack-on-saudi-oil-firm-disquiets-us.html?pagewanted=all

44 Ibid

45 Forbes (2012). The world's biggest oil companies. Retrieved from http://www.forbes.com/pictures/mef45ggld/1-saudi-aramco-12-5-million-barrels-per-day/

46 Encylopedia Britannica, (2013). Aramco. Encyclopedia Britannica. Retrieved from http://www.britannica.com/EBchecked/topic/31594/Aramco

47 Reuters, (2012, Dec. 9). Aramco says cyberattack was aimed at production. The New York Times. Retrieved from http://www.nytimes.com/2012/12/10/business/global/saudi-aramco-says-hackers-took-aim-at-its-production.html

48 Perlroth, N., (2012, Oct. 23). In cyberattack on Saudi firm, U.S. sees Iran firing back. The New York Times. Retrieved from http://www.nytimes.com/2012/10/24/business/global/cyberattack-on-saudi-oil-firm-disquiets-us.html?pagewanted=all

49 GReAT-Kaspersky Labs., (2012, Aug. 16). Shamoon the Wiper – Copycats at Work. Securelist. Retrieved from https://www.securelist.com/en/blog/208193786/Shamoon_the_Wiper_Copycats_at_Work

50 Ibid

the product of a nation-state.[51] Even though Shamoon was not on the same level as Wiper, it is still an impressive piece of malware that was able to do damage to important systems. Whether it was the unimpressive work of a nation-state or the work of a skilled group of non-state actors, it made an impact and had an effect on Saudi Aramco.

These insights raise the question of whether or not this was an isolated attack by a non-state actor, or whether it was one in an ongoing series of salvos between the Iran and US cyber communities. Iran certainly possessed the motive – retribution for sanctions levied against it, and the cooperation by Saudi Arabia, a Sunni Muslim nation which has been at odds with Shiite Iran before. Typically, however, in an act of retribution the attacker invites attribution which Iran did not. Also, despite causing destructive action to the data on the computers, the virus did not attack the actual control systems and as a result did not manage to damage oil production. The relative crudeness of the code and use of the term "Arabian Gulf" in concert with the insider knowledge of the hacktivist group "The Cutting Sword of Justice" and the use of an Aramco insider to facilitate the attack could suggest that it was simply a singular attack by a non-state actor.

Iran's doctrine is one of asymmetric and proxy warfare. It has been suggested that Iran used unofficial hacker groups such as the "Iranian Cyber Army" to both defend against and engage in attacks[52]. It is possible that "Arabian Gulf" was a red herring intended to further obscure the origin of Shamoon.[53] Using a proxy to launch an attack aligns with Iran's strategic culture but the exact author is not known. It is possible that Iran did not wish to engage in direct conflict, but intended to make the sanctions less viable by ensuring Aramco would be unable to supply the necessary volume of oil. If this were the case then the attack would show a severe flaw in Iran's understanding of the oil production systems by not attacking the control systems, instead, which should be unlikely due to Iran's own expertise in oil production; or it may have been intended to send a message advertising the capability while not crossing a direct line by inflicting significant infrastructure damage. This, however, is pure speculation and not empirically derived analysis. If Iran did in fact orchestrate the Shamoon attack, it would suggest that the series of attacks on Iranian critical infrastructure were followed by retaliation on the American oil supply chain. This would indicate an ongoing and escalating conflict that should be cause for concern.

51 Ibid

52 Rezvaniyeh, F., (2010, Feb. 26) Pulling the strings of the net: Iran's Cyber Army. PBS. Retrieved from http://www.pbs.org/wgbh/pages/frontline/tehranbureau/2010/02/pulling-the-strings-of-the-net-irans-cyber-army.html

53 Perlroth, N., (2012, Oct. 23). In cyberattack on Saudi firm, U.S. sees Iran firing back. The New York Times. Retrieved from http://www.nytimes.com/2012/10/24/business/global/cyberattack-on-saudi-oil-firm-disquiets-us.html?pagewanted=all

AN INCIDENT OF NOTE

One incident which appears on the list is singular in that unlike the other noted events it does not appear to be the result of a direct cyber-attack: the Deepwater Horizon oil spill. On April 20th, the culmination of severe neglect of safety protocols and a slew of design and implementation flaws incurred the worst environmental disaster in US history. [54] While drilling the Macondo well in the Gulf of Mexico, the Deepwater Horizon oil rig had a "blowout" in which an uncontrolled mixture of mud and gas was released after failure of pressure control systems. The gas spread across the rig and is believed to have first ignited in the engine room, initiating several explosions and causing the rig to eventually be engulfed in flames and sink.[55] The reason the "Deepwater Horizon" event appears on a list of "cyber-related oil industry events" is because, regardless of the cause, the incident had several failures in networked control and safety systems which could have prevented the catastrophe from occurring after the blowout.

The former chief electronics technician on the rig, Michael Williams, noted during testimony before a government panel that the alarms which would notify the crew of a gas situation was placed in an "inhibited" mode for over a year because "they did not want people woke up at 3 o'clock in the morning due to false alarms [sic]."[56] Additionally, other monitoring and control systems intermittently froze, and a fire and alarm system was set to "override active." Despite a series of four tests conducted in the hours before the incident to ascertain that the integrity of the well, no alarms were sounded or reported directly before the incident. These control issues solidify the idea that there was a cyber-component to the catastrophe. When taken into the context of other events which occur in and around the same time period, it becomes clear that though there is no direct evidence pointing to a malign threat actor's involvement, such an attack is technically viable.

It is incredibly unlikely that any state or non-state actor was involved in an attack on the Deepwater Horizon; however the circumstances preclude the exclusion of this possibility, remote though it may be. The Blowout Preventer (BOP) was recovered and forensically examined, but most other evidence cannot be examined – it has either ceased to exist or is inaccessible. The destructive nature of the accident and the apparent corporate neglect makes collecting any cyber-forensic evidence linking the incident to an actor infeasible. Most evidence is destroyed, unusable, or largely inaccessible at the bottom of the ocean. It is likely that any control system audit reports or logs capable of providing insight either would not have attributed anomalous activity to an unidentified APT, or would not be comprehensive enough to provide evidence that could retroactively suggest an APT. The audit logs themselves are dubious due to allegations that Transocean and BP were hastily rushing procedures because of large scheduling overruns.[57] Further allegations have surfaced against BP employees and contractors accusing them of destroying evidence in the wake of the disaster.[58] Bearing in mind that there is no direct or forensically sound evidence and that only circumstantial evidence is available, the vignette which will now be explored is the use case of the Deepwater Horizon incident as a cyber-attack.

Several events that have occurred both before and since the BP oil spill suggest that an attack would be technically feasible. According to an article attributed to Dorothy E. Denning, a professor of computer science at Georgetown University, in 1992 a disgruntled former employee of Chevron intentionally disabled alarm systems at Chevron's oil refineries for 10 hours by "hacking into computers in New York and San José, California."[59] While this only affected on-shore refineries and is dated enough that technical controls may have improved since then, another attack in 2009 showed that control systems on off-shore rigs may be also disabled remotely. Mario Azar, a disgruntled contractor formerly working for Pacific Energy Resources, sabotaged an offshore oil rig "computer system that PER used to communicate between its

54 (David Barstow, 2010)
55 (How the Rig Crew Responded to the Blowout, 2010)
56 (Investigation of Deepwarer Horizon Explosion, Mike Williams, 2010)
57 (Drilling, 2011)
58 (Affairs, 2012)
59 (Denning, 2000)

offices and its oil platforms. The computer system also served a 'leak detection' function for PER."[60] The systems were disabled from May 8th until June 29th before it was noticed.[61] And as recently as February 23rd 2013 an article in the Huston Chronicle stated that "Malicious software unintentionally downloaded by offshore oil workers has incapacitated computer networks on some rigs and platforms, exposing gaps in security that could pose serious risks to people and the environment."[62]

These articles would seem to state that a cyber-attack on an off-shore rig is not only possible, but a reality. Complicated control system attacks such as Stuxnet have already proven that even in conditions where network access is unavailable, intelligent viruses can still perform a predetermined function at a designated time. By extension of these occurances, it may be concluded that a capable attacker could manipulate safety control systems of an oil rig from shore, and do so through a sophisticated control system virus which can operate even when not in contact with a C2 server.

If it is assumed that Deepwater Horizon was an attack, it gives rise to the question of attribution. In order to attribute an attack for which there is no direct or forensic evidence, one must instead turn to political attribution. This includes considering which actors had the motive, means, and the opportunity to perform the attack. Motives can in part be divined through observation of the direct and indirect outcomes of the event and its beneficiaries. After narrowing the scope of actors, one may then examine the policies, strategic culture, operations, and tactics of relevant actors against different dimensions of the event to reveal alignment or correlation.

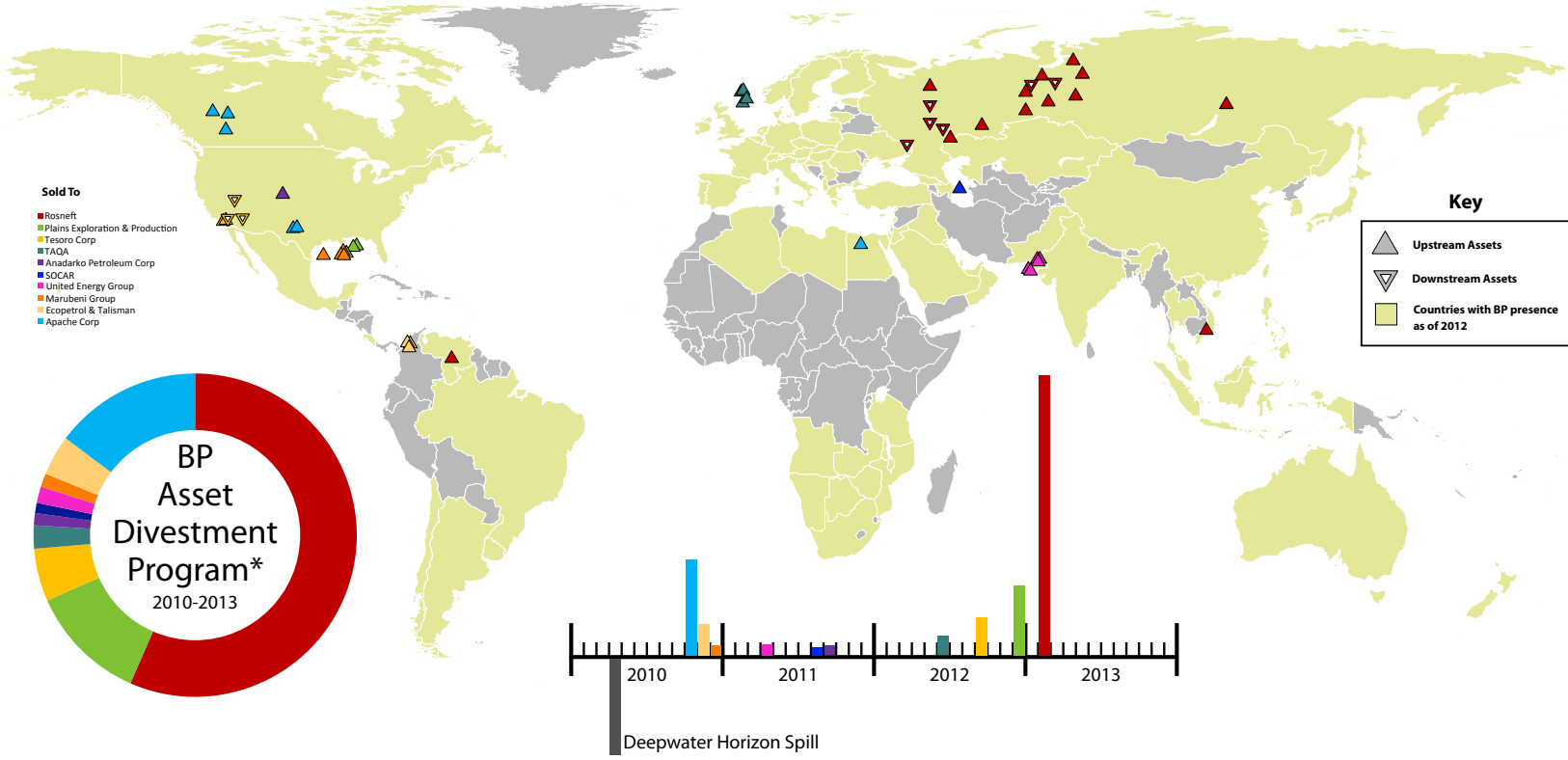
Immediate and direct impacts of the Deepwater Horizon oil spill were as follows:

- A moratorium on any drilling in the Gulf of Mexico for the ensuing 6 months
- The Macondo well becoming unusable, at least in the immediate
- Ecological disaster in the United States and other GoM adjacent countries
- Heavy political damage, fines, and charges levied against both BP and contractors such as Transocean, Ltd.

BP has been by far the biggest figure attached to the incident. As of March 2013 BP has been forced to spend or provision $40 Billion as a result of Deepwater Horizon.[63] To put this in perspective, BP's combined profits for the years of 2010-2012 amount to about $34.6 billion.[64]

These impacts in and of themselves are notable, but they also created a ripple effect of indirect consequences as well. These indirect outcomes include the possible fluctuation in oil and gas prices and potential for geopolitical fallout from the ecological disaster. Additionally though, and perhaps most significantly, in 2011 BP announced a $38 billion asset divestment program in order to cover the costs of the enormous fines incurred by the Deepwater Horizon spill.[65] So what did BP divest, and to whom?

60 (Mrozek, 2009)
61 (United States of America v. Mario Azar, 2009)
62 (Shauk, 2013)
63 (Williams, 2013)
64 (BP, 2012, p. 34)
65 (BP, Financial and Operating Information 2007-2011, 2011, p. 3)

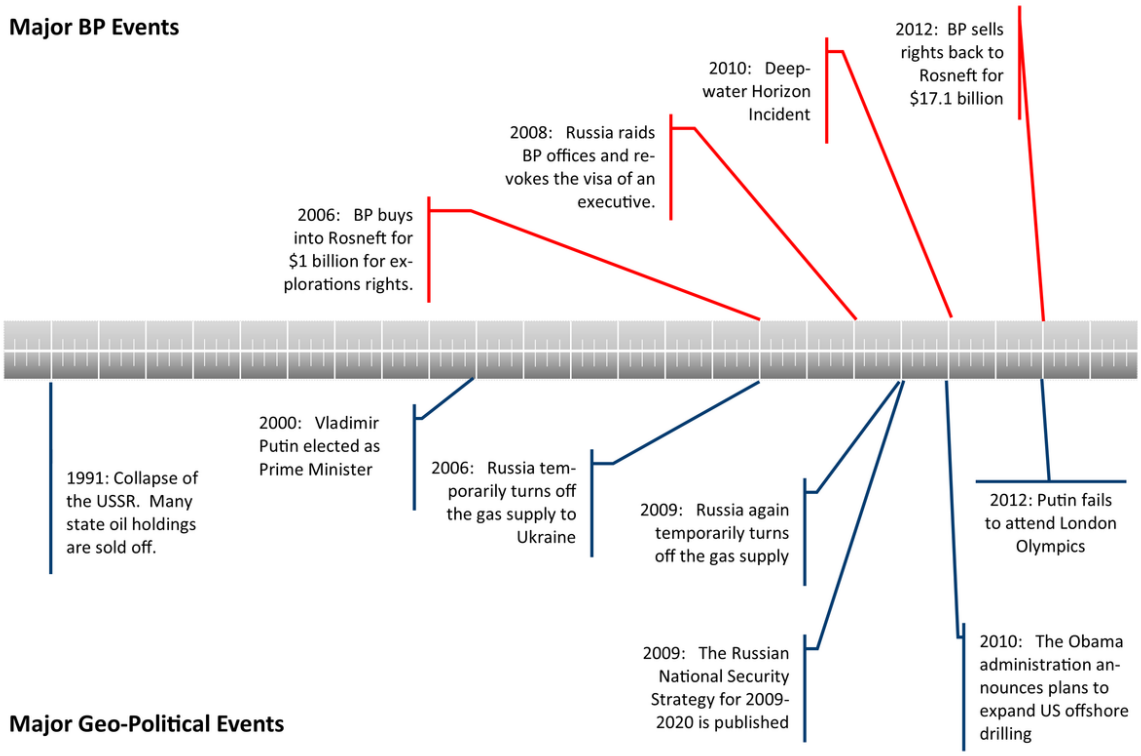


This data would suggest that one of the main beneficiaries of the oil spill is Rosneft, a state-owned oil company belonging to a state actor which possesses both a cyber-capability and vested interest in the oil industry. It is the only one of the top five oil producing countries yet to be mentioned: the Russian Federation. In July of 2012 Forbes released an article on the World's largest oil companies. What was notable about the article was this quote: "But when sorting through the rankings of the World's 25 Biggest Oil Companies and looking at who controls and influences the biggest of big oil one thing becomes clear: no industry leader has more sway, has twisted more arms or made more deals than Russian President Vladimir Putin." The article goes on to point out the Russian President's past use of Gazprom—the state-run oil giant and second largest producer in the world—as a political tool and his vast influence over other non-Russian oil companies. Russia, an acknowledged force in cyber and the second largest exporter of oil in the world, is markedly absent in the last decade from the master timeline either as an aggressor or as a target, barring of a few leaked emails by the Anonymous hacking group. This appears aberrant, even despite the possible language barrier mentioned at the beginning of this report or Russia's tightly controlled dissemination of information.

While clearly the Russian Federation was the largest beneficiary of BP's post-spill divestments and also benefited from a halt in Gulf of Mexico oil production, the question that remains is whether or not the possible acquisition of TNK-BP (which would be difficult to predict) is motivation enough to engage in a risky enterprise such as a cyber-attack that results in a kinetic outcome—particularly when weighed against the possibility of direct attribution that could have far reaching implications to relations with both the UK and the US. If these benefits alone are not enough, then what other motivators existed which, in concert, would have been cause for Russia to launch a cyber-attack on a UK company operating in the Gulf of Mexico? In order to properly answer these questions many factors need to be examined, including:

- the extent of BP-Russian relations leading up to and beyond the Deepwater Horizon incident
- Geopolitical considerations of the time
- Any competition in market-share between BP and Russian state-controlled oil companies
- Russia's overall relation to and dependence on the oil industry
- Russia's strategic goals at the time
- A high-level understanding of the Russian approach to cyber warfare

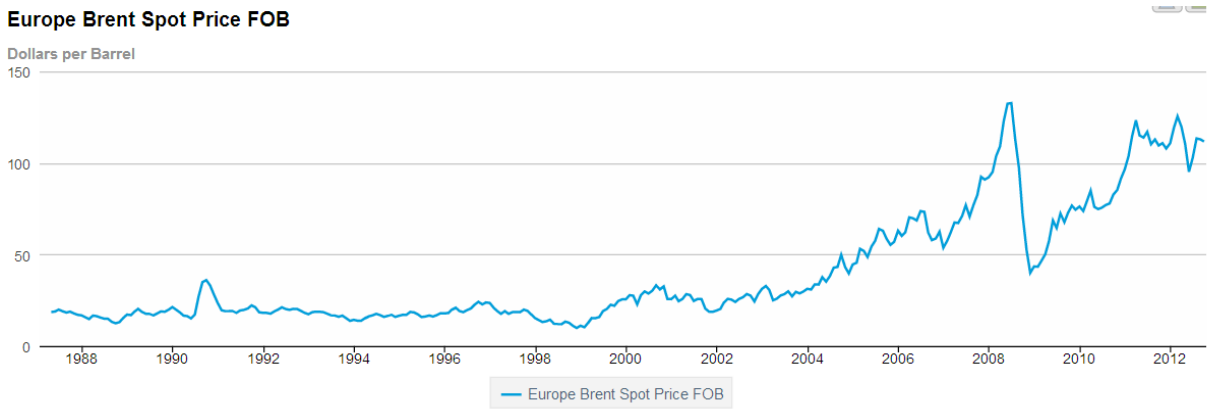
An interesting relationship between Russia and BP has unfolded over the past decade, revealing a series of exchanges that highlight a tenuous co-existence. The figure below displays this in detail, aligned with geopolitical events. The exchange begins in 2006 when the Russian state-run gas company Rosneft went public on the London stock exchange and BP purchased 1 billion in shares. This is a seemingly straightforward strategic partnering; however there was speculation that BP was "pressured into investing in order to secure future oil exploration rights for its own Russian joint TNK-BP."[66] Robert Amsterdam, a layer for the former head of Yukos (an oil company absorbed by Rosneft), was quoted as saying that BP "has a gun held to its head."[67] Then in June 2007, The Russian government pressures BP to sell one of the world's largest natural gas fields to state-run Gazprom or lose the license to develop it.[68] 2008 presented perhaps the height of tensions when armed police raided BP-TNK's Moscow offices[69] in what appeared to be an effort to intimidate shareholders. This came on the heels of speculation that Russia wished to "buy out the shareholders of TNK-BP as part of its campaign to tighten control of the country's energy assets."[70] In a related vein, the BP-TNK CEO was forced to leave the country after Russian authorities refused to renew his visa.[71] Also in 2008, an important BP incident which did not appear to directly involve Russia occurred. Off the coast of Azerbaijan at the Central Azeri platform in the Caspian Sea, one of BP's off-shore rigs suffered a blowout nearly identical to that of the Deepwater Horizon. The gas did not ignite, and no one was killed, however it did cost around $50 Million a day in losses for the Azeri government. BP purposefully kept all details of the incident under close wraps verging on a cover-up. Then the Deepwater Horizon event occurs in 2010, followed by the sale of TNK-BP to Russian state-run Rosneft in 2012 as part of the asset divestment program initiated to pay for the spill. In that deal, BP also purchased shares in Rosneft, upping their stake from 1.25% to 20% and receiving two seats on the board of directors, including one which was awarded to BP's current CEO Robert Dudley—the same gentleman who was forced to flee in 2008 over an un-renewed visa. However, according to a Reuter's article published on March 4th of this year "…as a state appointee, Dudley would have to vote by government directive on major issues, such as large deals and key appointments." [72] This remark is in contrast to another individual who had "been nominated as an independent and as such can decide for himself how to vote." [73]



66 (Kennedy, 2006)
67 Ibid.
68 (Kramer, 2007)
69 (Hodgson, 2008)
70 Ibid.
71 (Webb, 2008)
72 http://uk.reuters.com/article/2013/03/04/uk-bp-rosneft-idUKBRE92310W20130304?feedType%3DRSS%26feedName%3DbusinessNews
73 Ibid.

These Russia-BP relations coincide with an amalgam of geopolitical events not directly related to BP, but offering supporting context for eventual conclusions drawn about the Deepwater Horizon oil spill. Following the collapse of the Soviet Union in 1991, many of the state owned oil and gas assets were sold at significantly discounted values to private individuals creating an economic void for a fragile new country already plagued by monetary issues in other sectors. Russia faltered economically for most of the 1990's until Vladimir Putin was elected President in 2000 under a banner of planned economic prosperity. Putin is an interesting figure, and has played prominently in Russia's return to the world stage. A former KGB member, Putin has sought the consolidation and reclaim of critical sectors of the Russian economy, most notably the energy sector. Using strong-arm tactics and political pressure, he has set the tone for Russia's future policy. In 2006, Russia temporarily turned off the gas it was supplying to the Ukraine, inciting conflict and unrest with other European countries. The move was cast as an overt attempt to regulate natural resource prices for a market in which Russia controls production and reaps profits from a customer base with limited alternate supply. Russia used the tactic again in 2009, shutting off gas supplies for two weeks to Ukrainian Naftogaz ostensibly because of a dispute over contract terms which had been negotiated in 2002 regarding the appropriation of gas by Naftogas. The ordeal was only resolved after Ukraine's Prime Minister sat down with Vladimir Putin and renegotiated a new contract for Russian gas, for which she later received a 7 year sentence on charges of abuse of power.

These events serve to highlight the importance Russia places on the energy sector as both a vital portion of its economy and a potent political tool. The Russian economy is heavily dependent on the oil & gas industries, with 62.7% of its economy being service based industries in 2010.[74] Many economists have pointed to oil and gas prices as the Achilles heel of the Russian economy.[757677] This was made evident in 2008 when oil prices plummeted (as seen in the figure below), sending the Russian economy spiraling into a recession. Prices hit a low in 2009, one year before Deepwater Horizon and at a time when reports were also stating that the overall output of Russian oil for 2010 was projected to decline.[78] This stagnation in the economy combined with future projections of slowed oil production presented a huge threat to Russia, and it is likely that this sentiment resonated with Russian authorities. As pointed out by a Forbes columnist, a sustained drop in oil prices like that in 2008 would mean possible civil unrest and political instability – oil and gas have that magnitude of effect.[79]



This resonance may perhaps be seen in the Russian National Security Strategy to 2020 published in May of 2009. The document outlines a path for Russia to continue to regain prominent global power, and within it there are several points which lend credence to a strategic view of oil and gas resources. The document states that "the longer-term focus of international politics will concentrate on the possession of energy resources, notably in the Middle East, on the Barents Sea shelf and other areas of the Arctic, in the Caspian Sea Basin, and in Central Asia."[80] The same publication

74 CIA Factbook 2012

75 http://www.forbes.com/sites/kenrapoza/2012/04/03/oil-a-problem-for-russian-economy-official-says/

76 http://www.ssb.no/a/publikasjoner/pdf/DP/dp617.pdf

77 http://oilprice.com/Energy/Crude-Oil/Putin-Plays-Down-Russias-Deadly-Dependence-on-Oil-Gas-Revenues.html

78 http://www.reuters.com/article/2009/10/14/russia-oil-production-idUSLE70186320091014

79 http://www.forbes.com/sites/markadomanis/2012/12/01/russia-and-oil-a-recipe-for-preservation-of-the-status-quo/

80 Thomas, T. (2011). Recasting the Red Star. *Fort Leavenworth: Foreign Military Studies Office*. ,p.87.

also states that "the competitive search for resources does not exclude the use of force." [81] Force in this case does not necessarily indicate a military kinetic action, but exertion of both soft and hard power across all domains, including cyber.

What follows is a purely speculative narrative of one possible attack scenario, intended to highlight elements of Russian doctrine which align with aspects of the BP oil spill. It will also include techniques and tools which provide functionality that makes such an attack feasible.

So it is possible that after the oil price crash in 2008, Russian officials saw the danger to social and political stability in the country. Forecasts for Russian oil output around 2009 also suggested that not only were prices dropping, but overall production would as well, envisaging the specter of future unrest and hardship. Realizing the strategic importance of oil and the success they had garnered with previous market halts, they needed a way to either artificially inflate oil prices, increase demand for Russian oil, or increase oil output. It is worth noting that price of natural gas (another huge component of the Russian economy) is inextricably linked to oil prices in most of Europe during this period because gas is price-indexed against oil. Unlike the natural gas incidents where Russia was able to use state-controlled Gazprom to halt gas leaving the country, a sizeable portion of the oil leaving the country was from privatized companies. It would be difficult to overtly prevent them from exporting without significant backlash from international communities (such as the World Trade Organization where they had been seeking entry for some time), so action would need to be more covert. One of the largest of these private oil firms was TNK-BP, which Russian authorities had already attempted to strong-arm into government control as they had done with other smaller oil companies like Yukos. The other main exporter of oil to Western Europe at this time was BP plc, the 50% owner of TNK-BP. Therefore, control of TNK-BP would both increase oil revenues and state-output, and simultaneously decrease a prime competitor's overall output. It would also give them a larger political weapon that could be used as a bargaining chip or to meet the aforementioned goal of price control. However, BP had proven recalcitrant and defiant about relinquishing TNK-BP in spite of the pressures which had already been applied. A past rocky relationship with BP combined with their recent safety failures and cover-up in the Caspian Sea also made them a viable target.

If they could not be motivated by conventional means, then Russia would have to revert to force as pointed out earlier in their National Security Strategy to 2020 ("the competitive search for resources does not exclude the use of force"). Sabotage could be a viable option, however it would have to be on a large enough scale that BP would be put into a position where they would fold to Russian interests under the additional pressure. While an on-shore explosion would cause some delays in production and potential loss of life leading to litigation, off-shore destruction would have the potential to be significantly more damaging publicly, could also include loss of life, and would incur significant environmental fines in addition to safety fines.

The question would then be where to strike – BP holdings in the Caspian Sea would be too dangerous as any failures could easily implicate Russia and any success could cause collateral damage to Russian oil assets and coastal regions. The North Sea would be a potentially viable candidate with multiple countries being affected resulting in more economic impact on BP, however the currents are such that collateral damage could occur to other areas that Russia identified as vital fields of competition, namely the Barents Sea. BP's other major developments were in relatively new fields in the Gulf of Mexico (GoM) where BP planned to invest heavily. Russia has long seen (and continues to see) American power as a dangerous counter to its own, marking the US as its top global competitor. The GoM then would prove very attractive as it offered a two-fold bonus. A cash-strapped United States, riddled by its own recession, would bear the brunt of the collateral damage resulting in heavy fines to BP, perhaps made heavier because of the state of the American economy. Secondly, BP would possibly lose its asset(s) and right to drill offshore in the GoM, a region BP considered strategic. It would allow for an information influence operation on the American public – poisoning the market against BP, but also potentially against the American government if they repeated any mistakes in their handling of an incident like the 2005 Hurricane Katrina rescue and relief effort.

America in 2008 and 2009 was already facing internal contention over deep water drilling practices, meaning that a significant event in the region could perhaps halt production by governmental directive. Even with the contention, BP had already made history in the Gulf; in mid-2009 the Deepwater Horizon rig finished drilling the deepest oil well in history in the Tiber Oil Field off the coast of Texas. This meant that one of the top competitors for Russian oil exports was making headway in this region. America is also the largest importer of oil, so even though oil prices are a complicated affair that takes into account aspects like the economic stability of different regions and future projections of demand, any damaging effects on American production or supply could potentially increase oil prices.

In March of 2009, drilling of a new well, Macondo, was approved and scheduled to begin later that year, creating

81 Ibid., p.87.

an ideal target. Realistically, in a clandestine project of such importance it is likely that Russia would have identified several GoM targets, perhaps alongside BP North Sea assets as well. Having the Gulf of Mexico in mind, Russia now needed a method for delivery. Analyzing the 2008 incident in the Caspian Sea which was still fresh at this time, it may have been noted that one of the root causes of the blowout was a flaw in the concrete—concrete possibly provided by the same US contractor who worked for BP in the GoM: Halliburton. They may have also surmised that if the alarms and safety systems had not activated in the Caspian Sea incident, the crew may not have been capable of reacting quickly enough to prevent an explosion, thus creating a terrible ecological disaster and causing loss of life.

So, a workable option appeared to be a covert cyber-attack on rigs operating in the gulf which disabled safety measures or created a situation where a blowout would occur. If done correctly, they could easily hide any attribution behind China (who had been actively stealing secrets from oil companies at this time), a non-state hacking group, a sporadic virus, or merely a glitch/accident. Because of the high stakes involved in any attribution to Russia, the best option would be making it purely appear to be an accident or neglect by BP and its contractors. This could be achieved by playing on known patterns and behaviors by BP that were risky. The type of intelligence Russia would have been intimately familiar with through their own dealings with BP and analysis of other BP safety incident in the recent past. This blends seamlessly with the Russian concept of "Reflexive Control."

Timothy Thomas points out in his book entitled "Recasting the Red Star" the concept of reflexive control—as Timothy puts it: "Reflexive control is defined as a means of conveying to a partner or an opponent specially prepared information to incline him to voluntarily make the predetermined decision desired by the initiator of the action."[82] Purposefully setting false alarms off in the early hours of the morning so that someone will disable them would be a good example of this. Russian hackers such as the GLEG group have demonstrated proficiency in finding exploits in ICS software by releasing the Agora SCADA+ exploit kit which had a plethora of zero-day exploits in it.[83] This demonstrative proficiency, combined with the previously noted 2009 Mario Azar incident would suggest that the technical capability to set this in motion was readily available. After identifying several targets in the GoM, Russian operators could easily have exploited a multitude of attack vectors. Employee's personal systems (which could have VPN access to onshore control stations or the rig directly), mobile devices like smart-phones, portable storage devices such as usb drives, engineer laptops, or an onshore control center with access to the rigs could have been leveraged to gain access. Such attacks could be trivially done even with open-source or free tools such as the iconic Metasploit Framework. Metasploit's custom payload, Meterpreter, for example is capable of residing purely in volatile memory, often leaving few residual traces on persistent storage, if any. After identifying an entry point such as social engineering (perhaps too high profile) or more likely exploitation, Russian operatives could find a series of servers at the onshore control center with a long up-time or that were not regularly updated (and therefore not regularly restarted). The attackers could have leveraged these to create redundant avenues of access which run entirely in volatile memory, thus leaving minimal to no permanent traces. More likely and stable however would be the use of such exploitation to install a persistent backdoor. From here they could have stolen credentials or otherwise escalated privileges to gain access to the safety systems on the Deepwater Horizon and other rigs operating in the area. It is likely that the same attack vector would not have been used in every instance to obscure any pattern analysis and diversify opportunities for success. At this point setting off alarms in the early hours to encourage employees to disable them, impairing other safety systems and causing general instability would have been enough to subtly magnify the effects beyond a manageable level resulting in catastrophe.

After having discussed in some detail the possibility of a state actor's involvement, it must equally be considered that there is also plenty of evidence suggesting that this was nothing more than a tragic incident. It may also be stated that there is evidence contrary to the posed scenario. The Deepwater horizon incident and the 2008 Caspian Sea incident before it were merely two incidents in an industry fraught with others. Additionally, two incidents—regardless of similarity—are not conclusive enough to represent a pattern. Should they be a part of a larger pattern, it is far more likely that these particular incidents pointed to a pattern of corporate neglect than anything else. The inherently dangerous nature of oil refinery work would imply that accidents and loss of life are an unfortunate reality of the industry. According to the Centers for Disease Control and Prevention, "The fatality rate for oil and gas workers in the U.S. between 2002 and 2007 was more than 29 deaths per 100,000 workers, or about seven times the average for all occupations."[84] BP is no stranger to such hazards. Deepwater Horizon, though perhaps their worst to date, was not their first prolific disaster. BP was required to pay 1.6 billion dollars in victim compensation for the Texas City refinery explosion from March 23, 2005. They were also required to pay 50.6 million dollars in fines for failing to fix the safety violations that were brought

82 Recasting the Red Star

83 https://ics-cert.us-cert.gov/pdf/ICSA-11-096-01.pdf

84 Centers for Disease Control. (2013, March, 3). Retrieved from http://www.cdc.gov/niosh/programs/oilgas/risks.html

to them by OSHA before the explosion.[85] These same corporate failings were present in the Deepwater Horizon incident and were brought up during the senate hearings. This in part serves to highlight the fact that even if the incident were to be a state-sponsored attack, the impact of the loss of a single rig or small well is relatively inconsequential to the overall oil production of the victim. The timeline of the Deepwater Horizon incident also speaks volumes – the incident took place over the course of at least a year and was the product of many budget-saving decisions that were acknowledged to be dangerous by the engineers who were working on the Macondo well drilling effort. These measures and a culture of risk are likely what ultimately sealed the fate of the Deepwater Horizon. These occurrences are too intricate whilst spread over such an extended period of time for any one entity to have reasonably controlled them all.

It is within human nature to look for a pattern or design for an event even when there isn't any – this can be augmented by time as more possible "clues" become apparent. For this reason such attribution which seeks out a conclusion is a slippery slope and must be approached with caution—it has a tendency to entice analysts to find facts to fit the hypothesis as opposed to a hypothesis which fits the facts. It's important to remember that correlation does not equal causation; in fact correlation may be coincidental or the result of another unanticipated factor. Likewise the circumstantial evidence alone is not conclusive. Between 1969 and 2005 there have been over 30 separate incidents on oil rigs ranging from fires and explosions, to structural failures, some of which were blowouts not unlike the one that occurred on Deepwater Horizon. It is likely that circumstantial information about one or more of these could be strung together to provide a reasonably convincing political 'attribution.'

Regardless of the attribution or refutation of an attack, the takeaway from the Deepwater Horizon analysis is that the oil industry is undeniably tied to the cyber domain and an attack on this sector is conceivable; that by using currently available cyber means a kinetic, violent, and instrumental outcome could very possibly be affected on a private sector by a foreign state actor or other human-based agent to gain a favorable outcome.

85 BBC News, BP agrees to pay record 50.6m fine for Texas explosion. (2010, August, 12) http://www.bbc.co.uk/news/business-10960486

CONCLUSION

The observation of a moderately sized cross-section of cyber events within the oil and gas industry clearly indicates that there is ongoing cyber conflict. This conflict exists in the form of espionage and sabotage, and it involves both state and non-state actors. In the case of cyber espionage, these actors are advanced in the sense that they have launched multi-year campaigns which have gone undetected as they have exflitrated what is likely untold billions of dollars in intellectual property. There tactics represent a formalization and ritualization of the conflict which will suggests that it has been weaponized and will continue to escalate in the future. The Chinese government is absolutely involved in some capacity, and stands to gain the most out if these transactions. China will need to continue to make aggressive moves to sustain its need for oil going forward as its ability to meet growing demand becomes overwhelmed. Red October, while largely targeted at diplomatic entities, also targeted the oil and gas industry. The sophistication of the infrastructure used in Red October, as well as the methods, suggest a revolution in the type of cyber conflict that will be seen in the oil and gas industry. A majority of these groups are still active as of April 2013, even after being outed in reports released by antivirus and incident response companies over the last few years. These reports themselves represent one aspect in which non-state actors will become ever more important in cyber conflict, particularly within important industries such as oil and gas. American companies are particularly vulnerable targets to state-backed or state-owned foreign competitors who may in the future leverage their countries' cyber forces to gain competitive advantage, or possible develop their own.

This type of competitiveness may lead to the types of sabotage exchanges seen in the Middle East. These attacks may either have been the work of nation-states battling out policy in the cyber realm, or unconnected events with the Shamoon attacks merely being a disaffected hacktivist group expressing dissent. Regardless of origin, these exchanges are clear examples of cyber conflict of a destructive nature. Going forward, the sophistication of the viruses used in these attacks will likely only increase. Attacks like the flame and Stuxnet viruses may be seen by American companies within the industry. The line between espionage and sabotage attacks can be somewhat blurred with viruses being modular and having the capability to perform both; gathering intel while waiting undetected to unleash a more sinister capability. The very use of these types of malware breeds and intimacy and familiarity with them that allows for their further proliferation by the parties who were previously attacked. Even if they cannot reverse engineer them, they may understand the behaviors well enough to crudely mimic them.

As discussed at the beginning of the paper, cyber conflict is attractive. It is attractive to criminal elements, corporate elements, individuals, hacktivists, state actors, and other sundry non-state actors alike. Because of its low barrier to entry, availability, and outsized impact, the oil industry must prepare for sustained future conflict in this realm.

APPENDIX A – DEFINITIONS

Advanced Persistent Threat: An advanced persistent threat (APT) uses multiple phases to break into a network, avoid detection, and harvest valuable information over the long term. These phases are Incursion, Discovery, Capture, and Exfiltration according to Symantec.[86]

Anonymous: A decentralized group of individuals who label themselves as "hactivists." The individuals are a non-state sponsored group. The group frequently picks their targets based on current events or decisions of companies that conflict with an ever changing mantra of the group. The attacks perpetrated by Anonymous are frequently not complex in nature and often are designed just to restrict access to public websites through a denial of service attack.

C2: Command and Control

Cyber Warfare: "Actions by a nation-state to penetrate another nation's computers or networks for the purposes of causing damage or disruption. "[87]

Dropper virus: A type of Trojan that serves to transport and extract a viral payload onto the destination system. The dropper is frequently made to masquerade as an innocuous executable that once executed the viral payload has been deployed. The dropper service at this point no longer needs to be running. [88]

Exfiltration: The opposite of infiltrate. The act of secretly stealing information from the enemy's control. It is a form of espionage.

Malware: A generic term used to describe software designed to cause malicious actions on a computer system. Trojans, Viruses, and Worms are examples of types of Malware.

Reflexive control: "A means of conveying to a partner or an opponent specially prepared information to incline him to voluntarily make the predetermined decision desired by the initiator of the action."[89]

SCADA: Supervisory control and data acquisition are a type of industrial control system usually deployed to monitor systems over long distances.

Spear phishing: The process of attempting, often through email, to acquire someone else's user information. This is achieved through social engineering and often involves sending emails that appear to be from a known and trusted individual.

Trojan: A type of computer malware that does not replicate, rather its primary function is to allow unauthorized access to the computer systems, steal information, or cause harm to the infected system. A Trojan often presents itself as an innocuous file thus tricking the user into executing.

Virus: A type of computer malware that is able to self-replicate and infect multiple systems. The replication is usually tied to a human interaction.

---

86 http://www.symantec.com/theme.jsp?themeid=apt-infographic-1

87 Clarke, R A and Knake, R K (2010). *CyberWar, the next threat to national security and what to do about it*. New York: Ecco/HarperCollins.

88 Symantec. (2012, April 26). *Trojan.Dropper*. Retrieved March 9, 2013, from Symantec: http://www.symantec.com/security_response/writeup.jsp?docid=2002-082718-3007-99

89 Thomas, T. (2011). Recasting the Red Star. *Fort Leavenworth: Foreign Military Studies Office*.