INVISIBLE ATTACKS

CNIT 58100 FALL 2013

AUTHORS:
(listed alphabetically)

Faisel Al-Askandrani
Eric Amos
Joe Beckman
Nikhil Boreddy
Brian Curnett
Chris Martinez
Kelley Misata
Fillipo Sharevski
Hans Vargas

Under the Direction of Dr. Sam Liles

Purdue University
Cyber Conflicts and Transnational Crimes - CNIT58100 - Fall 2013

ABSTRACT

The movement of people and goods around the world is certainly no easy task and is heavily reliant on the intricate maneuvering of systems, processes, people and more than ever, technology. These systems to move the shipment of goods and transportation of people are critical to the world economy; particularly to the over 315 million people living in the United States.[1] The importance of shipping and transportation infrastructure to the United States is reflected in the inclusion of this infrastructure on the Cyber Infrastructure and Key Resources (CIKR) list created and maintained by the United States federal government. According to the Bureau of Transportation from 2009, this multi-trillion dollar industry consists of maritime, aviation, and ground transportation systems including road and railways; all of which are at the core of transportation operations.[2]

The world's growing reliance on advanced information technology has introduced opportunities for cyber attacks that exploit vulnerabilities in the information technology enabled systems. This report analyzes documented cyber attacks on the shipping and transportation industry and discusses the potential impacts of that analysis on U.S. shipping and transportation infrastructure.

(1) United States Census Bureau. (2013). U.S. and World Population Clock. Retrieved from http://www.census.gov/popclock/
(2) Bureau of Transportation Statistics. (2009). *Transportation Commodity Flow Survey*. Retrieved from http://www.rita.dot.gov/bts/sites/rita.dot.gov.bts/files/publications/pocket_guide_to_transportation/2012/html/table_04_06.html

EXECUTIVE SUMMARY

"We count on computer networks to deliver our oil and gas, our power and our water. We rely on them for public transportation and air traffic control... But just as we failed in the past to invest in our physical infrastructure - our roads, our bridges and rails - we've failed to invest in the security of our digital infrastructure... This status quo is no longer acceptable - not when there's so much at stake. We can and we must do better."

President Obama, May 29, 2009

Goods traded within and among nations around the world are the lifeblood of the world economy and critical for every day life. The shipping industry transports trillions of dollars of goods per year to all corners of the world. Many of the same methods used to move tangible goods are also used to move people - safely, securely and with great speeds. Consequently, the shipping and transportation industry is an important target on which malicious actors can wreak havoc.

The application of information technology to this industry has added efficiencies and capabilities to the industry that would have been impossible a few years ago. This same technology has also fostered vulnerabilities in transportation systems that threaten nearly every aspect of its infrastructure. Easy to exploit, these vulnerabilities do not require highly skilled threat actors or vast resources.

The nature of information technology allows a wide variety of malicious actors, individuals, small unorganized groups and deeply rooted organizations alike, to inflict damage and cause disruption of mass proportions to systems. This asymmetry means that, through the technology and the Internet - the fifth domain of attack, cyber - a nation can be vulnerable to individuals or small organizations that, alone, would not have posed a threat in the past. This report is based on the guidelines of the United States Army: Open Source Intelligence (OSINT) analysis framework to clearly define the threats and impacts of cyber attacks, and sets forth a plan to mitigate threats in this fifth domain to shipping and transportation infrastructures within the United States and relevant around the world.[3]

(3) Presidential Policy Directive. (2013). Presidential Policy Directive -- Critical Infrastructure Security and Resilience. *Critical Infrastructure Security and Resilience*. Retrieved October 11, 2013, from http://www.whitehouse.gov/the-press-office/2013/02/12/presidential-policy-directive-critical-infrastructure-security-and-resil

EXECUTIVE SUMMARY

[continued]

While the cyber domain provides an attack space where superiority in physical resources and kinetic power can be defeated by an otherwise inferior enemy, well-resourced attackers may choose this domain as an alternative to other more visible or undesirable channels. The Stuxnet virus that destroyed Iranian nuclear centrifuges, which was widely attributed to the United States and Israeli governments, serves as an example of the use of the cyber domain by well-resourced agents. (4) Though other methods of disrupting the Iranian nuclear program were possible, cyber attack achieved the same goals without loss of life or positive attribution to either government. Consequently, the Iranian government was left with no one on which to take retribution, little justification to do so, and the attacker escaped international condemnation. Because of the challenges to attribution inherent in the cyber domain, this report will consider various types of actors.

Data collection methods and recommendations for cyber threat mitigation are broadly focused. The data referenced in this report has been gathered from global open sources, while recommendations for threat mitigation focus on critical transportation infrastructures of the United States.

These recommendations contain several key assumptions. First, it is assumed that no potential actor wishes to provoke upon themselves a kinetic response from the United States. With that said, again because attribution of actions to actors can be extremely challenging in the cyber domain, scenarios may arise in which an actor attempts to falsely attribute a cyber attack against United States interests to a third party, upon whom the United States directs a kinetic response. Second, it is assumed, based on this research, that the motives of potential attackers remain generally consistent with their motives in the recent past. For example, where some malicious actors have viewed it as beneficial to kill large numbers of American civilians, it is assume that they will continue to do so. The reverse is, of course, also assumed. This assumption is made because motivations for cyber attack speak to the ideology of the attacker and there is no reason to believe that the ideologies of potential cyber attackers have fundamentally changed.

Finally, it is important to assume that not all of the attacks, information related to attacks, cyber defense models, or capabilities relating to transportation and shipping infrastructures around the world are available through open sources. Because every potential actor discussed in this document could benefit from the secrecy of such information, it is assumed that some information related to this topic has been successfully been kept secret.

(4) Nicolas Falliere, Murchu, L. O., & Chien, E. (2011). *W32.Stuxnet Dossier* (pp. 1–69). Retrieved from http://www.symantec.com/content/en/us/enterprise/media/security_response/whitepapers/w32_stuxnet_dossier.pdf

Introduction to CIKR of Transportation

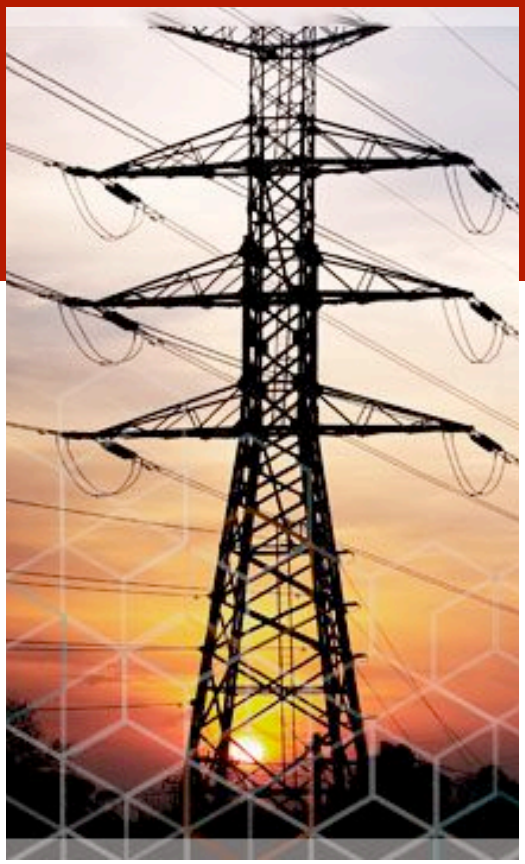
CIKR - Cyber Infrastructure and Key Resources

The devastation resulting from the terrorist attacks that shook the world on September 11, 2001 became a pivotal point in the way the United States and the world evaluate threats. In response, the United States established one of the most significant and overarching institutions in US history; the Department of Homeland Security (DHS). DHS has, among others, oversight responsibilities of agencies charged with securing the transportation and shipping infrastructures within the United States. Transportation is defined as land, air and railway systems, which is the focus of this research, though the CIKR of transportation includes others which are not included in this analysis.

The National Infrastructure Protection Plan (NIPP) has identified the transportation sector as one of the 19 U.S. critical infrastructure areas [(5)]. Sector Specific Agencies (SSAs) have the responsibility of securing each area, regardless of the distinctions between private and government sectors. The nation's transportation system, defined as "an expansive, open and accessible set of interconnected systems of airways, roads, tracks, terminals and conveyances that provide services essential to our way of life consists of six key subsections, or modes: (1) aviation; (2) highway; (3) maritime transportation system; (4) mass transit; (5) pipeline systems; (6) rail.[(6)]

"Our critical infrastructure - such as the electricity grid, financial sector, and transportation networks that sustain our way of life - have suffered repeated cyber intrusions, and cyber crime has increased dramatically over the last decade."

The United States White House (2011)



(5) Department of Homeland Security. (2013). https://www.dhs.gov/national-infrastructure-protection-plan

(6) Department of Homeland Security. (2013). *National Infrastructure Protection Plan for the Transportation Systems Sector* (Vol. 7, pp. 1–2). Retrieved from http://www.dhs.gov/xlibrary/assets/nipp-ssp-transportation-systems-2010.pdf

Introduction to CIKR of Transportation

CIKR - Cyber Infrastructure and Key Resources

[continued]

Figure 1 below illustrates the socio-economical significance of the transportation sector is supported by the Bureau of Transportation Statistics reference facts that the transportation related labor was 9.3 percent of the total labor force in U.S. in 2010, as well as the fact that the total value of the U.S. domestic freight shipments by mode in 2007 was 9.54 trillion dollars. On premise of this brief assessment, it is evident that the transportation sector, as one of society's vital functions, is a lucrative target for any actor that pretends to threaten, disturb or destroy the U.S. homeland security.

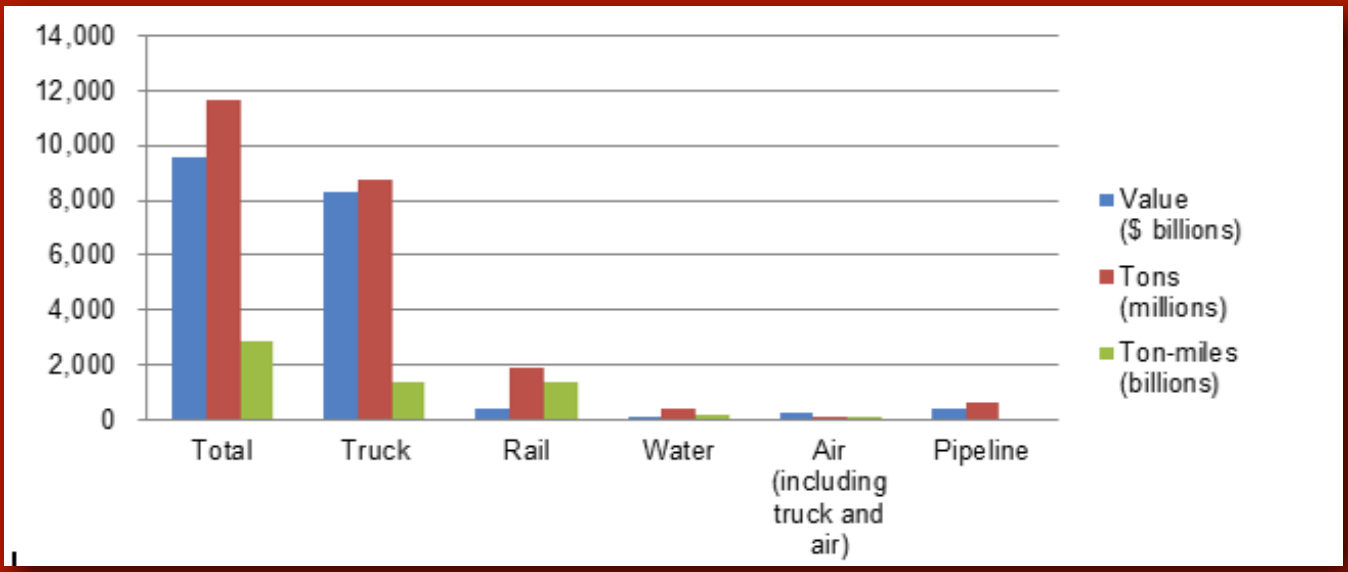


Figure 1 - Value, Tonnage and Ton-Miles of U.S. Domestic freight shipments by Mode: 2007. Adapted from Bureau of Transportation Statistics, 2009.

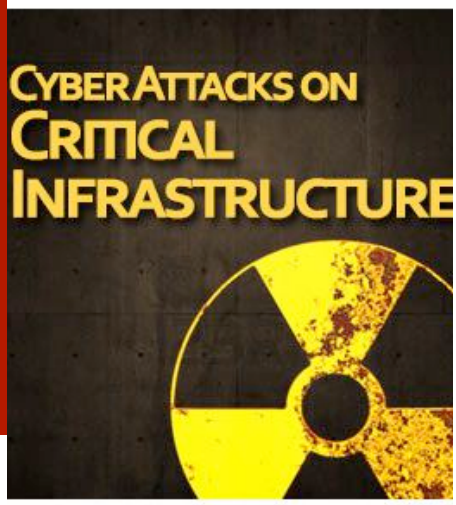
METHODOLOGY

The contents of this report were derived from the analysis of incidents reported through open sources which were caused by, or whose effects were intensified from, the use of cyber capabilities.

Open Source Intelligence (OSINT) was used to search and select the events included in this report.[7] The research team acknowledges that additional sources or events may have been overlooked or inaccessible; nevertheless the majority of the events presented in the following sections are relevant and sufficient in describing the extrapolate motives, means and opportunities to future cyber attack scenarios on critical infrastructures.

Attacks and vulnerabilities have been documented and organized in appendix section A. These events have been classified based on: attacker profile, motive, result of the incident, and by the identified target CIKR (Cyber Infrastructure and Key Resources) sector. Each incident was analyzed and discussed in-depth within the research team in order to identify the target profile, and the security vulnerabilities that were exploited. Incidents considered within this report are not limited to malicious cyber attacks. Included were vulnerabilities in the cyber domain identified by academic researchers, and accidents with ramifications within the domain.

"We face a menace that may represent the gravest short term threat to the peace and security of the human family in the world today."
Rep. Trent Franks, R-Arizona (2011)



Many other cyber attacks exist that have not been noted here. These attacks, often revealed through self reporting or through industry reports do not disclose highly important details of the exploit. Lack of disclosure also takes place at the nation-state level, where national sensitive networks or information has been compromised. Then further investigation and damage assessment takes priority over disclosure, although secrecy is not an unexpected reaction to these events. For the events the research team was able to find trustworthy sources, as registered on the respective references used throughout this document.

In order to group these event variables for effective analysis, classifications of the variables were standardized. Appendix A once again shows the resultant table of events with their seven classifying variables that are the basis for graphics and analysis in the next section of this report. The events, once classified, were evaluated against each of the seven variables listed above, and against the time of the attacks in relation to each other. After careful evaluation, conclusions about these events considerations were made to the particular context of each. From that analysis, the research team was able to draw conclusions about future threats against critical shipping, transportation infrastructure that would negatively impact the national interests of the United States.

(7) Handbook: US Army FMI Open Source Intelligence. (2008). Retrieved from http://www.fas.org/irp/doddir/army/fmi2-22-9.pdf

RESEARCH BIAS

As a direct result of the members of this research team being at an American academic institution, this report reflects those perspectives. The focus of the paper primarily being upon the infrastructure of transportation and shipping (and their sub-sectors) of the United States, the research team brings a strong approach from the perspective of an American academic institution into the analysis and conclusions reached in this report. The team recognizes potential biases from U.S. media sources and interpretations of world events received in the U.S.

Furthermore, because most of the incidents in this report were cited from western media outlets, western media biases may be reflected in this report. Research also reflects, in some respects the history, culture and experiences of the researchers involved. The research team comprised of 9 members representing 5 Countries - United States, Macedonia, India, Peru, and Saudi Arabia

Additionally, research and extrapolated scenarios in this report do no include personal transportation and ground traffic control systems.

Despite the body of evidence about to present from OSINT, the possibility of error is present as it is based on the information found, which could have been misreported or misrepresented out of context. The purpose, which achieved, was to find convincing evidence that the Transportation sector in the United Stated is under imminent cyber-attack.

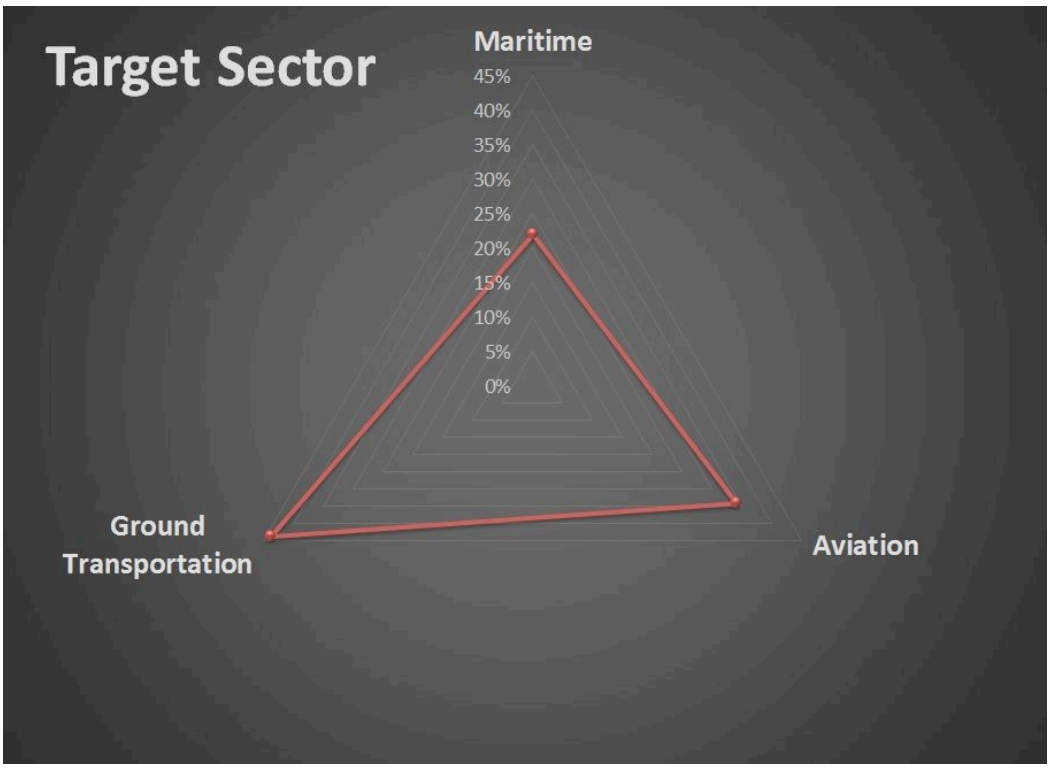
Cyber Incidents and Case Studies
CIKR of Transportation

In order to understand the current threats of cyber attacks agains the transportation sector of the CIKR (Cyber Infrastructure and Key Resources), the research team began by compiling incidents that occurred in the transportation infrastructures throughout the world; focusing attention on incidents which had a defined cyber component as a part of the reported incident. To provide greater organization in the research, each incident was reviewed and categorized by date, vulnerability vector, type of incident and primary actor suspected to be at the root of the incident. Each of these incidents and corresponding categorizations are detailed in the appendices following this report and compiled by percentage of occurrence in Figure 2 below.

Further analysis of these incidents are also illustrated in Figure 4 below. This figure marks the following 1. the nation state affected, 2. CIKR subcategory and 3. timeline of the incident as reported in the research.

Analyses performed on the incidents identified within the scope of this research shows a marked increase in the frequency of cyber events examined from 1995 thru 2013. Nevertheless, the evidence does not yield a clear pattern of attacks on the shipping and transportation industry that would place critical the infrastructures of the United States in imminent danger. Subsequently, cyber attacks on the global landscape within these industries are of valid concern particularly due to the dependency on emerging technologies, the exploitation of vulnerabilities becoming more visible, and the criminal enterprises (large and small in scale) continuing to make use of this infrastructure in the commission of crimes.

Figure 2



Cyber Incidents and Case Studies
CIKR of Transportation

[continued]

In short, cyber incidents related to the world's shipping and transportation infrastructure lack a clear pattern, but inform potential attacks, and can be used to focus U.S. offensive and defensive priorities.

Next steps in the research included taking a look through the lens of the attack vector, current technology capabilities allow for the use of never before imagined ease, accessibility and power of information and systems. Many of these capabilities make for a futile ground for malicious attackers to execute cyber-attacks. An example which is certainly plausible is the misuse of cloud computing resources to perform DDoS (Distributed Denial of Service) attacks by misrepresenting the credentials of an authorized user when signing up for cloud services, since then cloud providers continue to identify and learn from these attacks to strengthen their security controls including bandwidth allowances and services sign-up credentials authentication. (8) Another example of cyber of attacks utilizing vulnerabilities in the cloud is the use of botnets, which in sophisticated attacks compromise processing power of a computer system. Though too many other examples exist which are outside the scope and length of this report, it is important to emphasize that the attack vector is broad, deep and in a constant state of innovation which makes predicting and augmenting these attacks even more challenging for nation states around the world.

Additionally, a look from the attacker's vantage point it is, at times overlooked, but nonetheless important to consider the relevance of geographical location of the attacker to their mission for attacks. Many individuals or groups in this space enjoy the immunity sponsored by some countries or they see the value and importance in being distributed across several countries or continents. Both offer benefits and challenges which are worth considered further research beyond the scope of this paper. One example worth illustrating to this point of geographical importance came from researching to origins of attack traffic. As discovered in this research attacks of many varieties are easily originated from every corner of the world. Also, interesting to consider is the volume of these attacks from particular countries. Countries which already have a reputation for facilitating cyber threats or engaging threat actors.

In its latest "State of the Internet" report Akamai's, the world's largest distributed computing platforms, serving up to 20 percent of all web traffic 2013-Q2, Indonesia appears to be the top origination source for attack traffic based on IP address, becoming responsible for 38 percent of attack traffic. (9)

(8) Panja, B., Bhargava, B., Pati, S., Paul, D., Lilien, L. T., & Meharia, P. (n.d.). Monitoring and Managing Cloud Computing Security using Denial of Service Bandwidth Allowance. Retrieved from http://www.cs.purdue.edu/homes/bb/monitoring-cloud-security.pdf
(9) Akamai. (2013). *The State of the Internet*.

Cyber Incidents and Case Studies
CIKR of Transportation

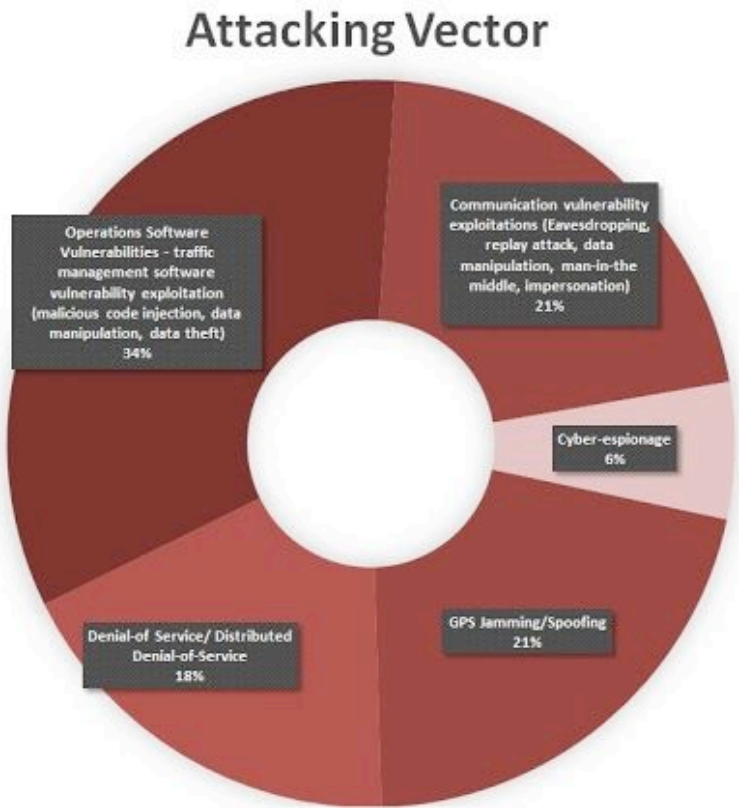
[continued]

Another example is offered by AlienVault's Open Threat Exchange data from its October 2013 report, identifying China as the holder of more malicious IP addresses than any other country in the world, followed after the United States.(10) The most common form of attack is the distributed denial-of-service (DDoS) attack, according to data from Arbor Networks, with the volume of high-bandwidth attacks steadily increasing.(11)

As cyber-attacks have become more common and, almost, expected in society's highly interconnected world, the geography and volume of these attacks has kept in lock step with the growing capabilities of the Internet and related technologies. To illustrate the vast spectrum of attackers Table 1, below, provides a synopsis by events researched of the of attacker profiles, documented or presumed motives and attack vector summaries. Figure 2 then offers a simple distribution illustration by attacker profile.

Figure 3 illustrates the results of the research team's analysis of the various attacking vectors.

Figure 3



(10) Blasco, J. (2013, October 16). OTX Snapshot: Top Malware Detected | AlienVault. Retrieved November 24, 2013, from http://www.alienvault.com/open-threat-exchange/blog/otx-snapshot-top-malware-detected

(11) Anstee, D. (2013, October 16). Q3 findings from ATLAS - Arbor Networks. Retrieved November 24, 2013, from http://www.arbornetworks.com/corporate/blog/5025-q3-findings-from-atlas

Cyber Incidents and Case Studies
Strategies, Tactics and Operations Analysis

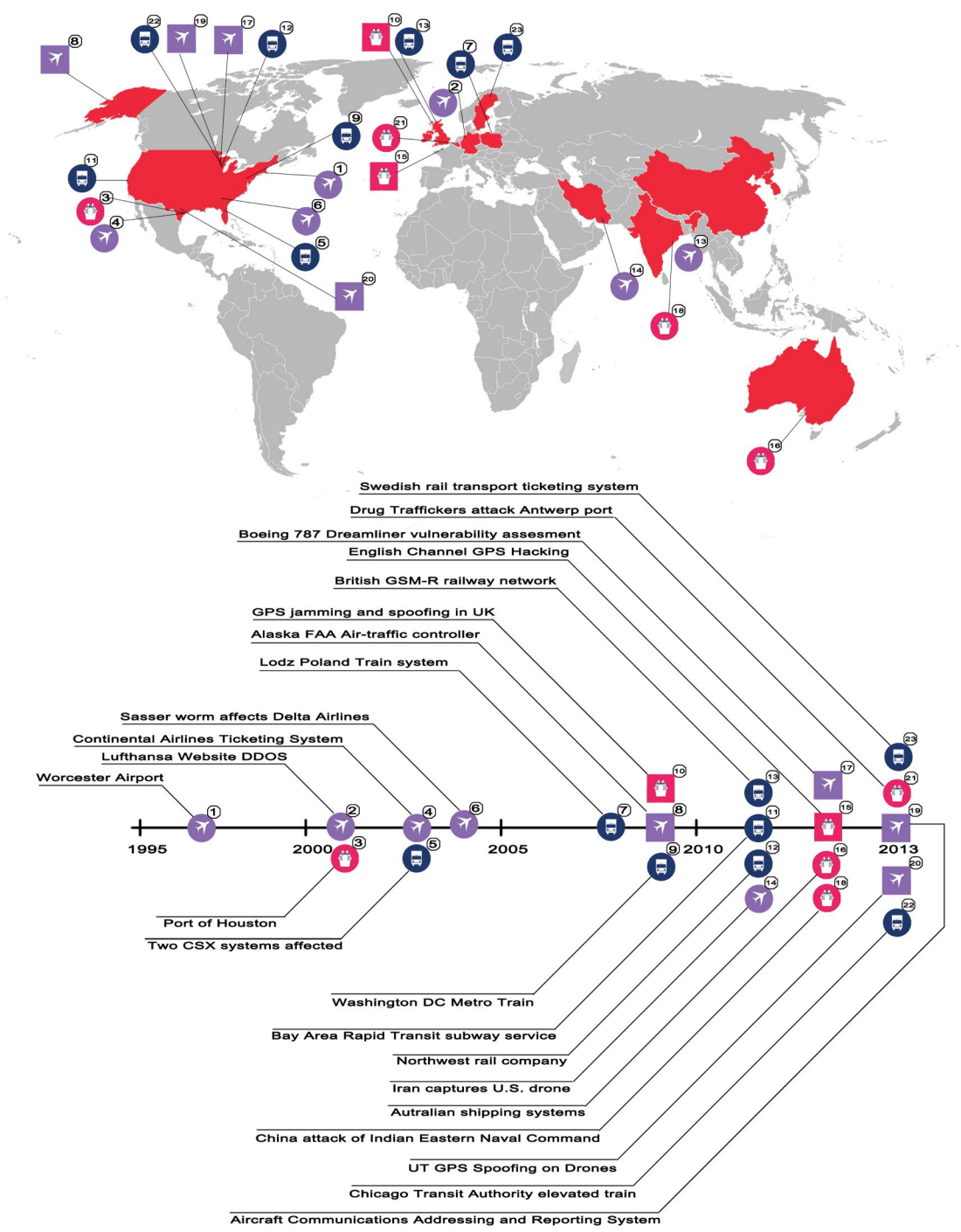


Figure 4: Timeline of Cyber Incidents and Case Studies:

As a first step toward understanding the series of cyber-attacks against critical infrastructures in transportation and shipping, the research team a chronological timeline of events was constructed and plotted on a world map. This global view illustrates the frequency of events from 1995 thru 2013.

Attacker Profiles
CIKR of Transportation

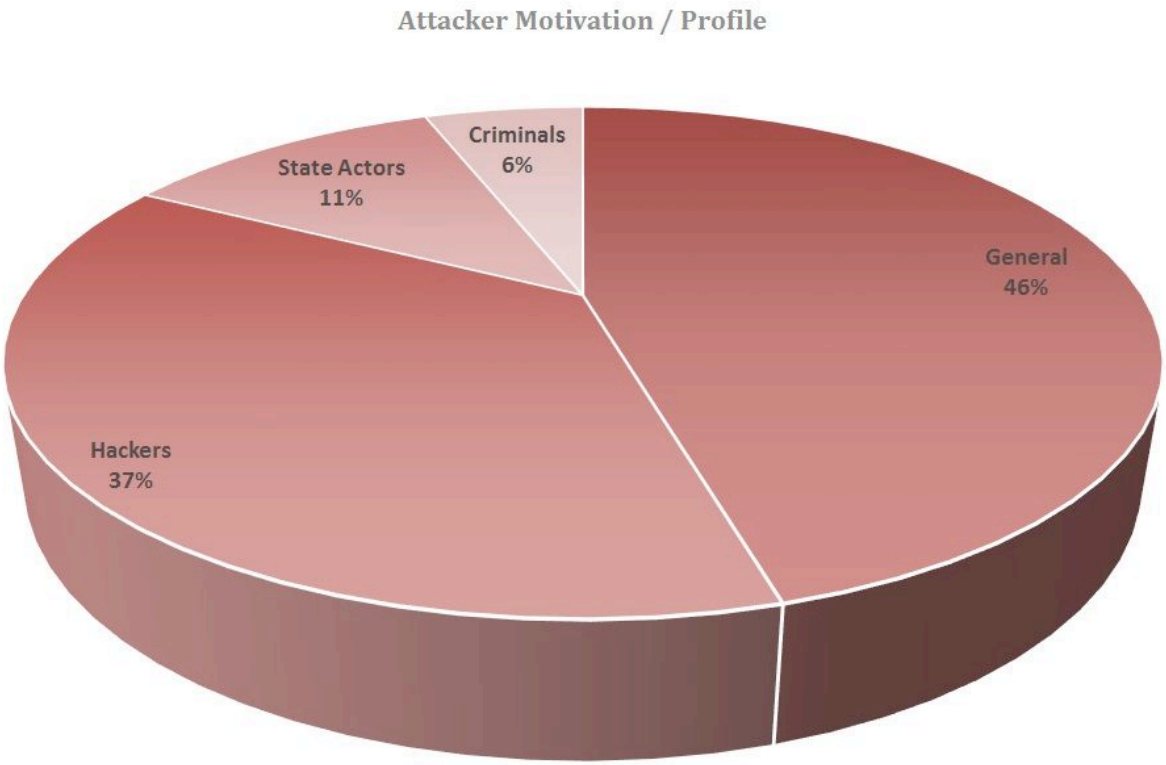
Table 1:

Event	Attacker Profile	Motive	Vector Summary
1	Hackers	Hacktivistm	Airport Air Traffic Control Telephone systems: disabled a loop carrier system, denying access to airport's control tower, fire department, airport security, and weather service, as well as private airfreight firms for six hours. Worcester Pharmacy
2	General	Hacktivistm	German airline Lufthansa AG said today that it successfully defended itself against a denial-of-service attack from demonstrators protesting the company's role in the deportation of illegal aliens
3	Hackers	Disruption	Aaron Caffrey, the 19-year-old who faced trial at Southwark crown court, was accused of hacking into the computer system of the second biggest port in the US.
4	Criminals	Disruption	Exploited a buffer overflow bug in Microsoft's flagship SQL Server and Desktop Engine database products
5	General	Unknown	The SOBIG computer virus, though not directed at CSX, infiltrated the rail company's world headquarters and brought down some of the company's communications systems. The degraded communications ability caused dispatching and signaling traffic delays that halted freight and passenger rail traffic including Amtrak service in Washington D.C. for a time.
6	General	Unknown	Computer worm known as Sasser infected critical scheduling systems at Delta Airlines, causing the delay and cancellation of several flights.
7	Hacker	Prank	A polish teenager allegedly turned the tram system in the city of Lodz into his own personal train set, triggering chaos. Jamming and altering the signaling part of the train dispatch system
8	Hackers	Disruption	In FY 2006, a viral attack originating from the Internet spread from administrative networks to ATC systems, forcing FAA to shut down a portion of its ATC systems in Alaska.
9	General	Terrorist	Due to poorly designed infrastructure two Washington DC trains collided in a head on collision. A fault in the computerized signal and operation system of the train network caused a failure to detect the two trains headed directly for one another and engage the automatic breaking.
10	General	Experimentation	GPS jamming and spoofing attacks on vessel navigation systems / experiment performed by the UK's Ministry of Defense on the THV Galatea.
11	Hackers	Protest	Members of the online hacktivistm group Anonymous have launched a 48-hour attack on San Francisco's Bay Area Rapid Transit (BART) subway service, launching their first salvo against the mybart.org website in the form of a few cyber-defacements and a massive data dump of users' emails, phone numbers, addresses, and login credentials.
12	General	Unknown	Computer hackers, possibly from overseas, infiltrated computer networks at Northwest rail company. The first infiltration caused schedule delays of 15 minutes. The second attack later in the day had no such effect.

Table 1 [con't]:

Event	Attacker Profile	Motive	Vector Summary
13	General	Experimentation	Train switching systems, which enable trains to be guided from one track to another at a railway junction, have historically been separate from the online world. GSM-R means they will be connected to the internet, however, raising the risk from Denial of Service attacks. The encryption keys are needed for securing the communication between trains and switching systems. They are downloaded to physical media like USB sticks and then sent around for installing - raising the risk of them ending up in the wrong hands.
14	State Actor	National Defense	The Iranian government captured an "enemy drone". The drone was later confirmed to be a U.S RQ-170 Sentinel drone by the U.S. government, who requested its return. Iran claims that it downed the drone using GPS spoofing techniques. The U.S. claims that the drone had other unspecified issues that caused it to crash. Additionally, the U.S. claims that its drones do not use GPS as their primary navigation method.
15	General	Experimentation	GPS jamming and spoofing attacks on vessel navigation systems / experiment performed by the UK's Ministry of Defense on the THV Galatea
16	Criminals	Drug Smuggling	The Australian shipping systems were affected by the hackers and drug dealers. They tracked all the ships with their containments. They found loop holes in the existing systems.
17	General	General	The ProASIC3 microchip, critical to the Boeing 787, drone aircraft, and other systems, contains a design flaw that allows it to be accessed from the Internet. This flaw is embedded into the chip and allows an Internet attacker to take control of flight controls.
18	State Actor	Intelligence	In an intrusion episode that occurred almost seven months ago, Chinese hackers penetrated computers at the Indian Eastern Naval Command to access strategic information.
19	Hackers	Research	Remote attack launched from an Android device can be used to take full control of an aircraft, using the Rockwell flight management hardware and software, Android application called "PlaneSploit" and an attack framework called "SIMON" that exploited the ACARS unencrypted communication link to upload an attacker controlled version of the flight management system. Once the attacker is into the airplane's computer, he is able to manipulate the steering of a (Boeing) jet while the aircraft was in 'autopilot' mode
20	General	Research	The University of Texas at Austin's Radionavigation Laboratory demonstrated hacking a civilian drone, forcing it to change course by sending fake GPS signals, Dr Todd E. Humphreys and his students did that. By doing so they recommended increasing the security of the navigation system by having it more spoof resistant, utilizing cryptography and other methods to authenticate the signature of the gps signal.the research is important since Congress ordered the FAA to come up with rules to allow government and commercial use of UAVs over American soil by 2015.
21	Criminals	Drug Smugglers	Police seized about one ton of heroin and the same amount of cocaine after being called in by shippers whose computer systems for following container movements had been hacked by drug traffickers.
22	General	Unknown	An out of service, and apparently unmanned Chicago Transit Authority elevated train passed through several track switches and accelerated to 20 mph before ramming another CTA elevated train full of passengers, injuring more than 30 people.
23	Hackers	Prank	A group of Swedish teens hacked the website of rail transport operator SJ. The teens produced a denial of service attack left customers unable to purchase tickets.

Figure 5: Distribution of Attacker Profiles



Target Profiles
CIKR of Transportation

To balance with the analysis of the attackers above, Table 2 below outlines once again by event, target profiles, vulnerabilities and a summary of the attack consequences.

Table 2:

Event	Target Profile	Target Vulnerability	Attack Consequences
1	Bell Atlantic computer system, disabled Telephone System	Vulnerability of the loop carrier system	Delayed air traffic for six hours. Exfiltration of data from Pharmacy.
2	Booking Website	Website resilience to DDoS	"Lufthansa denied that their was site offline for about 10 minutes by demonstrators sit-in efforts. German Website reported that Lufthansa's servers got 67,004 hits per second at one point in the two-hour Web attack."
3	Houston Port Authority Systems Arriving transporter ships	DDoS Vulnerability Exploitation	It froze the port's web service, which contained vital data for shipping, mooring companies and support firms responsible for helping ships navigate in and out of the harbor.
4	Attacking a known vulnerability in Microsoft SQL 2000 Web servers	Execution of arbitrary code on the SQL Server	Internet traffic worldwide: The slowdown was caused by the collapse of numerous routers under the burden of extremely high bombardment traffic from infected servers. Several routers
5	Train Dispatch and Control System	Email	Denial of e-mail service caused by massive message load.
6	Booking website	Windows Based Systems	Partial stop to operations
7	Train Dispatch Systems	Unprotected communication, legacy system components	12 injured, 4 trains derailed
8	Federal Aviation Administration: Air Traffic Control Systems in Alaska.	Web applications vulnerabilities. Software vulnerabilities.	FAA experienced an ATC outage for an unspecified amount of time.
9	Train Systems	Legacy systems	80 people injured
10	Maritime navigation systems (GPS part of AIS)	GPS signals susceptible to jamming, interference and spoofing	Vessel miss-navigation, sunk, hijack/hiding vessel presence
11	Web page defacement	Website vulnerability	ART's online services including web, mobile web, email and SMS unavailable on Sunday, August 14 from noon to 6.p.m.
12	Dispatch Systems	Unsecured SCADA controls	15 minute service delay
13	Railway communication system	GSM-R encryption keys vulnerabilities, GSM-R authentication and over the air communication	Service disruption, destruction and kinetic damage

Table 2:

Event	Target Profile	Target Vulnerability	Attack Consequences
14	GPS Spoofing	Iran claims that the system is vulnerable to GPS spoofing attacks. The U.S. denies this claim.	Iran now has U.S. advanced military technology that it can use to advance its own military capabilities. Iran also gains increased positive perception of its technical skills.
15	Maritime navigation systems (GPS part of AIS)	GPS signals are susceptible to jamming, interference and spoofing	Vessel miss-navigation, sunk, hijack/hiding vessel presence
16	Australian Customs and Border Protection Integrated Cargo System	Software vulnerabilities leaving the possibility for tracking the cargo through the port terminals	Tracking computer terminals through malware installed to gain access.
17	Plane Navigation System	Aircraft flight controls	Potential rerouting or destruction of the aircraft
18	Naval Submarine System	Systems bugs (unknown)	Data exfiltration
19	Air Traffic Control System, Aircraft autopilot system	ACARS/ADS-B lack of encryption and flight management system vulnerabilities	Change the plane's course, crash the plane, set lights flashing in the cockpit activate something when the plane is in a certain area, general service disruption, kinetic destruction and casualties.
20	GPS Spoofing	Un-encrypted Civilian GPS signals	Takeover drones and using it as missiles
21	Navigation and Surveillance Systems (Antwerp city)	Malware infection, remote access vulnerability - navigation and Surveillance Systems	Tracking computer terminals through malware installed to gain access.
22	Mass transit operating equipment and passengers	CTA operational control devices	More than thirty passengers injured and taken to area hospitals.
23	Ticket Purchasing Service	Ticket Purchasing Service	Passengers unable to use purchasing systems

Cyber Incidents and Case Studies
Strategies, Tactics and Operations Analysis

Classical construction of an organization is done in layers. In organizational literature, these layers are commonly classified as strategic, tactical and operational. The first layer, strategic, forms the top level of management and policy makers who are responsible for controlling the long range plan and development of the mission statement of the organization. The second layer, tactical, resides in middle management of the organization. Their focus is typically on the tasks that are needed to accomplish an objective(s) set by the operational level in the context of the overall strategic plan. Last, the operational level, are the day-to-day actionable tasks executed to achieve the tactical and therefore strategic plans of the organization.

A correlation of these concepts could be make when referring to cyber-attacks to the identified actors involved in attacks to the transportation sector of the CIKR within the United States. All the events identified in this research study could be described in terms of strategy, tactics and operations; however, when referring to these layers, the research team looked for implementations of these concepts as instruments to attack the transportation sector.

As a general synopsis of this research, the strategic element is identified to state actor and in some proportion with organized crime organizations due to a bigger picture planning, resource capabilities displayed, and benefits from a well executed attack, this attack could be also a forefront distraction to accomplish covert goals. The tactical level may set the tasks needed to accomplish the overall goal but they may not know what resources are needed to accomplish each task. At the operational level the members will assess the feasibility of each task given the availability of resources and the conditions at the time of setting the task. These feedback mechanisms are critical to accomplishing the long-term goal and a disruption at any level of the organization can cause extreme turmoil. This is what a potential adversary will try to do when attacking an organization.

Although risk exists in every evolution the risk is not realized unless an undesirable outcome occurs. When this undesirable outcome is not mitigated a successful attack occurs. When looking at the Strategic, Tactical, and Operational (with feedback) layer model, just like the fire triangle when addressing fires, when one of the layers is disrupted or communication is disrupted between layers a successful attack occurs.(12)

This can be accomplished kinetically or through cyberspace. General Colin Powell stated during Operation Desert Storm,

(12) Information about the Fire Triangle/Tetrahedron and Combustion. (2011). *Safelincs Ltd.* Retrieved November 19, 2013, from http://www.firesafe.org.uk/information-about-the-fire-triangletetrahedron-and-combustion/

Cyber Incidents and Case Studies
Strategies, Tactics and Operations Analysis

[continued]

"Here's our plan for the Iraqi army. We're going to cut it off, then we're going to kill it."(13) He was referring to the disruption of the layers of command and control dealing with the Iraqi Army's Strategic, Tactical, and Operational movements during the war. His staff was doing it kinetically, but the disruptions were deemed highly effective. Kinetic disruptions of this scale are highly overt and although effective might be seen as killing an ant with a hammer in some cases. Other situations might require something more covert. The same disruption can and has been achieved through cyberspace and how this was done will be examined.

In the case of Global Positioning System (GPS) jamming and spoofing this is an example of disrupting the Operational layer of the model. GPS work by acquiring satellites in space and using signals from these satellites to fix positions on or above the earth. By disrupting these signals or making a false signal more desirable than an actual signal the operational component of the model is still performed but with erroneous information. This information is then propagated through the rest of the command and control structure and incorrect information about a tactical unit's location is used causing a cascading failure in navigation. In this case the Integrity component of the CIA triad is also disrupted because there is no trust in the information received by the spoofed GPS signal. A Strategic layer attack against GPS might be to directly attack the satellites, by repositioning them or removing them. An attack against the Tactical layer of GPS would be to disrupt the satellites themselves, by having them spread false information throughout the whole GPS system, thus having a greater effect. Choosing one of these attacks over another is simply a matter of economics: if an exploit can be performed can be performed easier and cheaper than another then this attack will be performed.

Because of the proliferation of cyberspace certain kinetic attacks have been abandoned in favor of cyber attacks. Infamous bank robber Willie Sutton exclaimed when asked why he robs banks, "because that's where the money is."(14) This explanation gave rise to Sutton's law which simply states to look for the obvious.(15) Along those lines Sutton had probably encountered many situations that involved confrontations with security guards in banks. In entertainment a hostage situation in a bank is usually depicted as a criminal negotiating with law enforcement outside and a dead or wounded security guard on the inside. In 21st century banking it might go unnoticed, but no longer are there security guards posted in the lobbies of banks. Sutton's law might suggest that bank robberies are no longer occurring, but this would be false. These crimes have moved into cyberspace and because of it the actual risks of getting caught have decreased dramatically while the odds of success have increased.

(13) De Lama, G., & McNulty, T. (1991, January 24). Bush Says Desert Storm `On Schedule`. *Chicago Tribune*. Retrieved November 19, 2013, from http://articles.chicagotribune.com/1991-01-24/news/9101070715_1_cheney-and-powell-gen-colin-powell-pentagon

(14) Willie Sutton. (2013, November 11). In *Wikipedia, the free encyclopedia*. Retrieved from http://en.wikipedia.org/w/index.php?title=Willie_Sutton&oldid=581243459

(15) Sutton's law. (2013, May 30). In *Wikipedia, the free encyclopedia*. Retrieved from http://en.wikipedia.org/w/index.php?title=Sutton%27s_law&oldid=557575615

Campaigns of Cyber Aggressors
CIKR of Transportation

There are many potential cyber perpetrators behind the cyber-attacks and exploitation campaigns, each have different motivations and targeting profiles

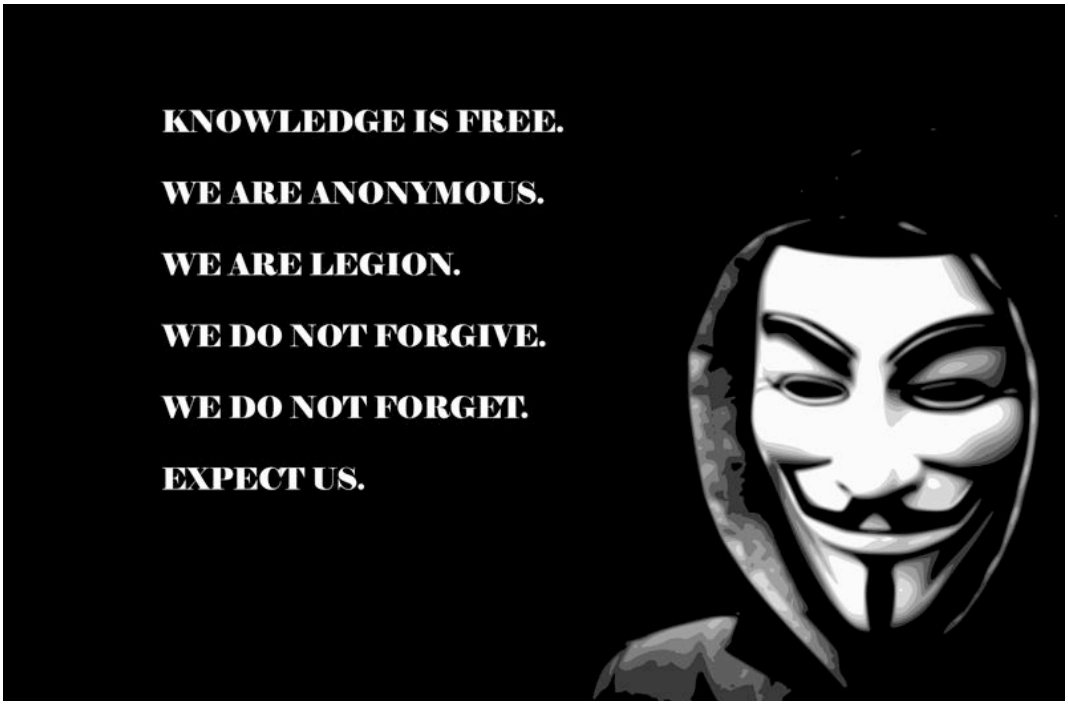
Country-sponsored warfare - National infrastructure attacks sponsored and funded by enemy countries must be considered the most significant potential motivation, because the intensity of adversary capability and willingness to attack is potentially unlimited.

Terrorist attack - The terrorist motivation is also significant, especially because groups driven by terror can easily obtain sufficient capability and funding to perform significant attacks on infrastructure. The terrorist is motivated by ideology and generally uses asymmetrical warfare attacks. Characteristics including: political motivation and loss of life

Commercially motivated attack - When one company chooses to utilize cyber attacks to gain a competitive advantage within it's market, it becomes a national infrastructure incident if the target company is a purveyor of some national asset. Characteristics including: data exfiltration, market sabotage and stock market manipulation.

Financially driven criminal attack - Identify theft is the most common example of a financially driven attack by criminal groups, but other cases exist, such as companies being extorted to avoid a cyber incident.

Hacking - One must not forget that many types of attacks are still driven by the motivation of malicious hackers; often spotlighted in the media as mischievous youths trying to learn or to build a reputation within the hacking community. This is much less a sinister motivation, and national leaders should try to identify better ways to tap this boundless capability and energy.



Campaigns of Cyber Aggressors
CIKR of Transportation

[continued]

Target CIKR sectors of interest for this analysis include the maritime transportation and shipping, aviation transportation and ground transportation infrastructures. A possible disruption of the normal infrastructure operation in maritime transportation potentially may cause a negative outcomes for the economic system that support, in terms of delay in the delivery of services and products. The concern is that the targets represent more than a valuable asset to the adversary; they are a valuable asset to the business, government agency, or applicable organization.

The fact that the transportation and shipping infrastructure support fragile economic markets (while also being insecure) make them even more valuable to terrorists. Because a nation can be easily destroyed (or debilitated) when these markets experience a hiccup or crash, they are also an ideal target for nation states looking to weaken another nation state. It is for these reasons that the targets (represented by the maritime industry) are a hot commodity. Nevertheless, the targets themselves, represent more than services and goods. They are the strategic, operational, and tactical backbone to our economy. As a nation reliant on transnational industries, its clear the lifeblood of the nation is dependent upon our ability to efficiently (and cost-effectively) transport materials. With the consistent increase in cyber adversaries (and the actualization of the targets to be exploited), it is essential that we understand (and emphasize) that the benefit for compromise is there for everyone and anyone. The important questions to consider include: Who exactly are the CIKR actors? How do they operate? What do they stand for? What are their objectives? What makes them so powerful?

Campaigns of Cyber Aggressors
Nation State and Country-Sponsored Warfare

Based on the incident reported relative to the actual cyber attacking campaigns initiated or linked to a state actor, the most employed attacking vector is the GPS jamming/spoofing (both for maritime and aviation), followed by a more classical intrusion and cyber espionage. It must be mentioned that none of these incidents can be categorized as entry point for further cyber conflict escalation between the involved state actors, or potential crisis initiation.[16][17] Rather than that, the GPS Jamming/Spoofing incidents may be seen in the context of potential cyber deterrence, and the may be seen in the context of cyber reconnaissance. [18][19] While these incidents might be considered as isolated low-intensity actions taken or supported by the nation state actors, a broader conceptualization together with the respective research cases studies are worth the attention from cyber-warfare strategic, operational and tactical perspectives.

The Peterson incident and the University of Texas research findings on GPS spoofing and drone hijacking by Storm on the other, indicate that any nation state actor might employ such a cyber attacking effort not just for cyber deterrence purposes, but as a first or retaliatory strike by "taking the control of the drones and using them as kinetic weapons."[20][21] Expanding the conceptualization of the nation state cyber campaign vectors beyond the domain of unmanned aerial vehicles, the potential exploitation of both the navigation and communication infrastructure and flight management systems for commercial aircrafts offer a plausible set of cyber attacking instances that might be utilized for military purposes.

(16) Lowe, M. (2012). Chinese hackers penetrate Navy's computer. Maritime Security Review. Retrieved November 10, 2013, from http://www.marsecreview.com/2012/07/intrusion- episode/
(17) Peterson, S. (2011). Iran hijacked US drone, says Iranian engineer. The Christian Science Monitor. Retrieved October 12, 2013, from http://www.csmonitor.com/World/Middle- East/2011/1215/Exclusive-Iran-hijacked-US-drone-says-Iranian-engineer-Video
(18) Lowe, M. (2012).
(19) Peterson, S. (2011).
(20) Storm, D. (2012b). Civilian drones vulnerable to hackers, can be hijacked, used as missiles. Computer World. Retrieved October 12, 2013, from http://blogs.computerworld.com/security/20593/civilian-drones- vulnerable- hackers-can-be- hijacked-used-missiles
(21) Storm, D. (2012b).

Campaigns of Cyber Aggressors
Nation State and Country-Sponsored Warfare

[continued]

In this direction, the attacks on the ADB-S, ACARS and BARR systems, the potential vulnerabilities of the Boeing 747-8, 747-8F and 787 Dreamliner aircraft, and the reported vulnerabilities of the FAA's MSSN systems open wide the possibility for the military actors to take control over both the commercial or government aircrafts by manipulating the communication and navigation interaction in order to disrupt/destroy the regular operation, or transform any flight to a potential kinetic weapon.(22)(23)(24)(25)(26)(27)(28)(29) Understanding that that these tactics can be combined with other operational instances and TTPs, would work toward the fulfillment of the strategic and operational goals of a nation state actor.

Conflating the consequence of the jamming attack together with the research outcomes relative to the GPS jamming/spoofing of the maritime communication/navigation, it is evident that some nation state actors have the capability to utilize cyber capabilities for cyber deterrence or for kinetic destruction. (30) (31) (32) Together with the GPS spoofing/jamming, the nation state actors might find it useful to exploit the Automatic Identification System (AIS) vulnerabilities as reported by as another possibility for kinetic distraction, or another channel for for cyber reconnaissance in the maritime domain.(33) Aside from the non-military maritime exploitations, the outcomes from the network penetration test performed on the U.S. Littoral Combat Ship (LCS) indicates a serious cyber exposures that make United States military maritime assets an attractive target for cyber exploitation in a broader context of warfare engagement. Should existing vulnerabilities be closed, opportunities to conduct low-intensity cyber intelligence abound. Through the creation of cyber information sharing organizations that resulted from the national effort to secure CIKR from cyber attack, industry sectors including the maritime. (34) These organizations are collaborations that catalog, notify, and attempt to guide the remediation of cyber security threats for their CIKR sectors.

(22) Schäfer, M., Lenders, V., & Martinovic, I. (2013). Experimental analysis of attacks on next generation air traffic communication. In *Applied Cryptography and Network Security* (pp. 253–271). Retrieved from http://link.springer.com/chapter/10.1007/978-3-642-38980-1_16

(23) Costin, A., & Francillon, A. (2012). Ghost in the Air (Traffic): On insecurity of ADS-B protocol and practical attacks on ADS-B devices. *Black Hat USA*. Retrieved from https://www.eurecom.fr/fr/publication/3788/download/rs-publi-3788.pdf

(24) Hoffman, D., Rezchikov, S. (2012). Busting the BARR: Tracking "Untrackable" Private Aircraft for Fun & Profit. DEFCON 20.

(25) Teso, H. (2013). Aircraft Hacking. In *Practical Aero Series*. Retrieved from http://conference.hitb.org/hitbsecconf2013ams/hugo-teso/

(26) How to Hack Into a Boeing 787. (2008, February 20). *FoxNews.com*. Text.Article. Retrieved October 14, 2013, from http://www.foxnews.com/story/2008/02/20/how-to-hack-into-boeing-787

(27) Fogarthy, K. (2011). Is it really possible to hack a 747's engines in-flight? IT World. Retrieved October 12, 2013, from http://www.itworld.com/security/223843/it-really-possible-hack-747s-engines

(28) Aero News Network. (2010). FAA Tells Boeing To "Hack Proof" 747-8, -8F. Retrieved October 12, 2013, from http://www.aero-news.net/index.cfm?do=main.textpost&id=c54094a8-d6cd- 404f-82d6-5598267eea23

(29) King, L. C. (2011). Quality Control Review on the Vulnerability Assessment of FAA's Operational Air Traffic Control System. Retrieved from http://trid.trb.org/view.aspx?id=1104102

(30) Espiner, T. (2013). THV Galatea trial. ZDNet Security. Retrieved October 11, 2013, from http://www.zdnet.com/uk-sentinel-study-reveals- gps-jammer- use-3040095106/

(31) Maritime Accident. (2010). GPS Hacking May Sink Ships. Retrieved October 11, 2013, from http://maritimeaccident.org/2010/02/gps- hacking- may-sink-ships/

(32) Maritime Accident. (2013). GPS Hackers Put Shipping In A Jam. Retrieved October 11, 2013, from http://maritimeaccident.org/2012/02/gps-hackers-put-shipping-in-a-jam/

(33) Guarnieri, C. (2013). Spying on the Seven Seas with AIS. Information Security. Retrieved November 10, 2013, from https://community.rapid7.com/com munity/infosec/blog/2013/04/29/spying-on-the-seven-seas-with-ais

Campaigns of Cyber Aggressors
Nation State and Country-Sponsored Warfare

[continued]

By creating these organizations, the industry sectors have created not only a collaborative body for protection, but have also created a vulnerability. Membership requirements for entry into these organizations are generally low, and are especially low within the maritime CIKR. Through membership, nation state actors seeking to exploit the maritime sector would have access to the current reported vulnerabilities, information about firms within the industry, and current thinking within the industry regarding cyber threat assessment. Actors with access to this information can utilize specific details to choose the tactics and targets that would most effectively accomplish their needs. These needs, oftentimes, represent the goal of destruction in these systems. Evidence of this can be seen in recent attacks listed in the appendix of this document.

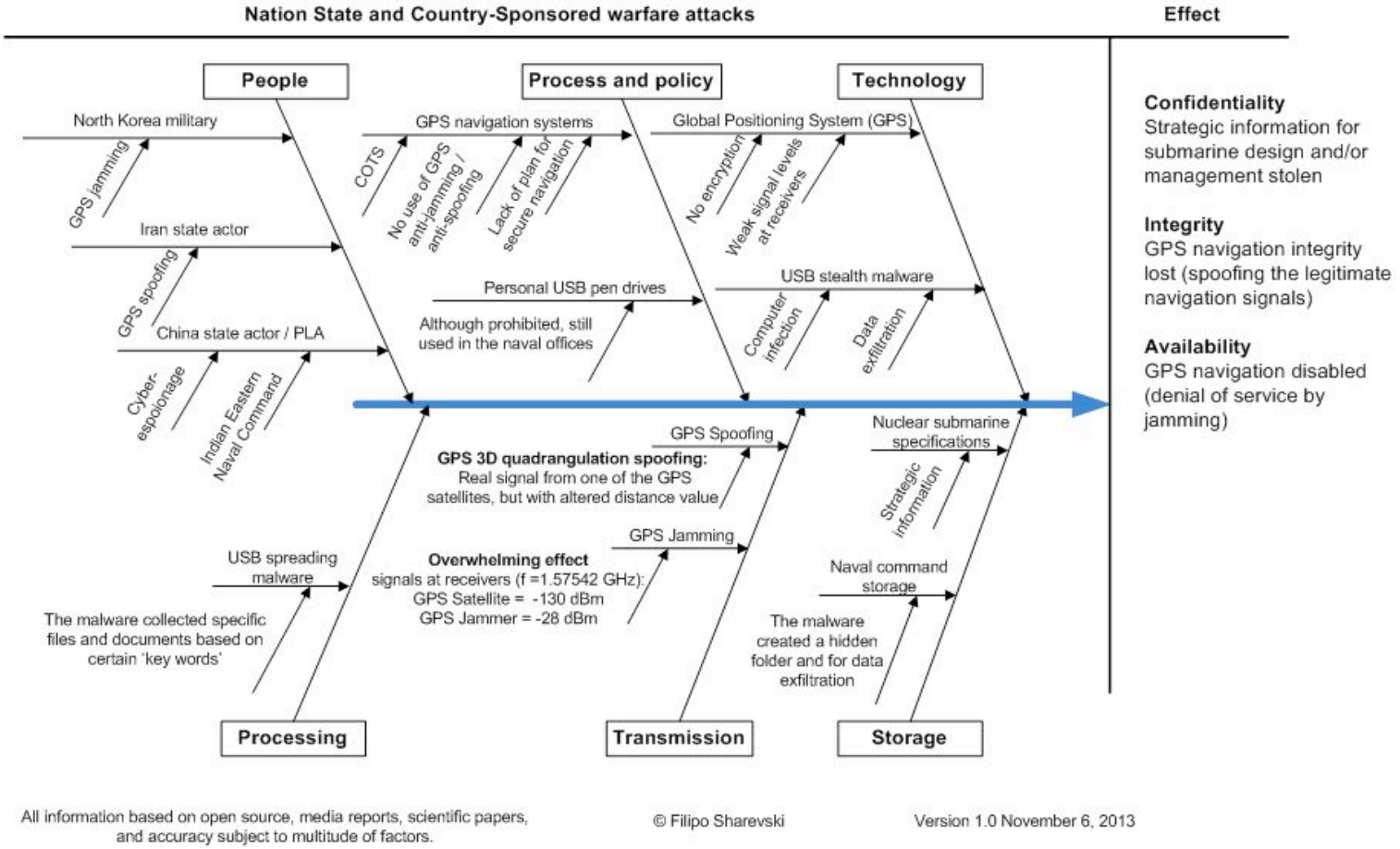
The attractiveness of the cyber exploitation component, together with its easy instantiation, makes it a critical weapon that any nation state actor seeks to have within its military arsenal. The actual evidence for the broad application of the general cyber exploitation techniques in each of the CIKR sectors of transportation clearly indicates that any nation state actor seeking to establish strong cyber warfare capabilities will utilize this potential for gaining considerable advantage in all of the war-fighting domains - not just within the cyber domain.

Campaigns of Cyber Aggressors
Nation State and Country-Sponsored Warfare

[continued]

The Ishikawa diagram below details the effects of nation state and country-sponsored warfare attacks on people, process, technology, processing, transmission and storage in relationship to the effects regarding confidentiality, integrity and availability in a cyber attack scenario.

Figure 6:



All information based on open source, media reports, scientific papers, and accuracy subject to multitude of factors.

Version 1.0 November 6, 2013

Campaigns of Cyber Aggressors
Terrorists

In the past, terrorist activities in the United States have broadly been motivated through the effective use of fear. Groups, often referred to as "EcoTerrorists", actually target CIKR for the purpose of stopping the development of projects that they feel may damage the natural environment. Because these groups seek to raise awareness for their causes rather than instill fear into populations, they will not be considered terrorists by the definition used in this section. Rather, the research team defined terrorists as those seeking to instill fear and murder innocent people. As a consequence of their motivations, terrorist organizations are less likely to focus on attacking the shipping and transportation CIKR where goods and freight are involved, and most likely to focus on points where large amounts of people are congregated. In our discussion of likely terrorist targets within this sector, time will be spent on air travel, maritime, and passenger rail systems. It is important to remember, however, that shipping and transportation tend to share infrastructure. The ability to impact multiple aspects of the segment with one attack makes an attack on shipping and transportation CIKR highly appealing to all potential attackers, including terrorists.

It is also important to note that the U.S. National Infrastructure Protection Plan (NIPP) specifically references protection against terrorism as a primary goal of the plan, and does not mention any other specific type of actor. This reference implies that the focus of the Department of Homeland Security as it relates to U.S. infrastructure is protection of infrastructure from terrorism. Also noteworthy within the Shipping and Transportation section of the NIPP, is the focus on defending against kinetic attacks, almost to the exclusion of other means of attack. If the threat of terrorist attack against CIKR is as large as the DHS indicates in the NIPP, and if the Shipping and Transportation Sector working group is focused almost completely on prevention of kinetic attacks, then the United States remains vulnerable to a terror attack of similar or greater magnitude via cyber as the kinetic attacks that security experts have spent so much time and treasure to prevent.

In order to translate the terrorist strategy into operational plans, the focus is on the places within the shipping and transportation CIKR sector that, if attacked, would create the greatest effect while using the fewest resources. In response to the terror attacks of September 11, 2001, attention to the air transportation sector of the United States and around the world grew exponentially. With that increased attention, terror attacks on this sector of American CIKR became much more difficult. Though there are cyber vulnerabilities in aircraft themselves, many physical and procedural safeguards exist that, although they would not prevent exploitations of cyber vulnerabilities

Campaigns of Cyber Aggressors
Terrorists

[continued]

within aircraft, they would likely prevent the attack from causing mass casualties. The recent publishing of exploited vulnerabilities in Aircraft Communications Addressing and Reporting System (ACARS) air traffic communications system by Hugo Tesco suggest that a cyber attack on such systems could produce a terror attack of great efficiency. However, Tesco attacked only a publicly available simulation version of ACARS software; so it remains questionable that ACARS attacks could produce an effect worth the effort.(34)

Maritime transportation is an enticing terror target because ships (especially cruise ships) concentrate thousands of people in a relatively confined space. Adding to the efficiency of the attack, several possible attack scenarios exist in open source documents, which should aid in making such an attack more easily. What likely deters terror attacks on cruise ships are increases in physical security in response to past hijackings, and the fact that most cruises host many passengers from very diverse nationalities. Killing so many people from so many different countries would reduce support for the actor by generating negative sentiment in most nations of the world. Further, crippling the cruise industry does relatively little economic harm to the United States compared with potential attacks on other aspects of the U.S. CIKR. For these reasons, terror attacks on maritime transportation in the United States is not the most effective option for organizations, and should not be the primary focus of prevention resources. However, possibility that terrorists may not use the maritime ISAC to gather cyber intelligence in order to operationalize attacks on the maritime sector if they have a plausible reason for doing so will be revealed.

An attack on the public transport system in the United States may best operationalize the strategy of terror organizations. Urban public transport provides a concentration of people that would maximize the effect of the attack with minimal resources. Proper placement of this type of attack could also minimize casualties of non-U.S. Citizens, and maximize other preferred demographics of the casualties. Terrorists can use incidents in Washington D.C. in 2009 and Chicago in 2013 as models to produce cyber attacks that would be difficult to stop.(35) It would kill a lot of people, both on the trains, and possibly in surrounding buildings, severely harm the American economy by reducing productivity by moving people away from public transport and onto crowded roads, and ruin critical infrastructure such as: rail lines, water supply, sewer, telecommunications, and electrical supply. An attack on urban light rail public transport that paired cyber and kinetic means, carefully selected, could serve the strategy of terrorists most effectively and efficiently.

(34) Teso, H. (2013)

(35) National Transportation Safety Board. (2010). NTSB CITES TRACK CIRCUIT FAILURE AND MATA'S LACK OF A SAFETY CULTURE IN 2009 FATAL COLLISION. Press Release. Retrieved October 13, 2013, from http://www.ntsb.gov/news/2010/100727c.html

Campaigns of Cyber Aggressors
Terrorists

[continued]

In order to translate the terrorist strategy into operational plans, the focus must be on the places within the shipping and transportation CIKR sector that, if attacked, would create the greatest effect while using the fewest resources.

Even when following their daily routine Liquified Natural Gas Carriers represent a grave threat to everything around them. Due to the energy content of the natural gas that they carry, many agencies and organizations have recognized the explosive potential. (30) Many ports and the companies that own these tankers maintain an exclusion zone around each tanker and pipelines are laid far out into the port as to keep the tanker away from populated areas.

The physical risk of the detonation of these LNG carriers has been heavily documented by the Department of Defense. (36) According to Sandia National Laboratories, these ships are prime target for a terrorist take over. In the event of a moderate leak, this concentration can be reached quickly at distances close to the source of the leak. Only 5% fuel air concentration is needed to detonate the fuel, meaning that a leak can quickly escalate into an explosion.To cause the fuel to vaporize all that is required is that the tanks be punctured in a large enough manner to render the cooling system ineffective. However, another option that is less documented is to attack the SCADA systems behind the cooling system. A cyber attack would turn off or down the cooling mechanisms while still showing normal functionality to the operators of the tanker. This attack combined with GPS spoofing could bring a ship within range of a heavily populated city and detonate without ever actually putting an operative on board the tanker. There are mechanisms in place to compensate for the destabilization of the fuel source. However, with a volatilized source such as natural gas this would only make the ship more dangerous under a hybrid cyber and conventional attack as seen within the Sandia Report Although an attack on an LNG tanker has not yet happened, the potential destruction from a cyber only attack or a hybrid based attack on a tanker is of grave concern.

Due to the extreme risk of these tankers and the exclusion zone policy put in place, It is possible to manipulate these tankers into traveling into areas restricted to them through GPS spoofing. It would also be possible to keep tankers in restricted areas for extended periods of time through communications jamming. The effects of this would be economic in nature. By moving these tankers closer to shore, policies in place should cause a complete and total shut down of the port and depending on the perceived intent of the tanker, an evacuation. (37)

(36) Hightower, M., Gritzo, L., Ragland, D., Luketa-Hanlin, A., Covan, J., Tieszen, S., et al. (2004). Guidance on Risk Analysis and Safety Implications of a Large Liquefied Natural Gas (LNG) Spill Over Water. Sandia National Laboratories,SAND2004(6258). Retrieved October 15, 2013, from http://www.osti.gov/scitech/biblio/882343

(37) Pitblado, R. M., & Woodward, J. L. (2011). Highlights Of LNG Risk Technology.Journal of Loss Prevention in the Process Industries, 24(6), 827-836.

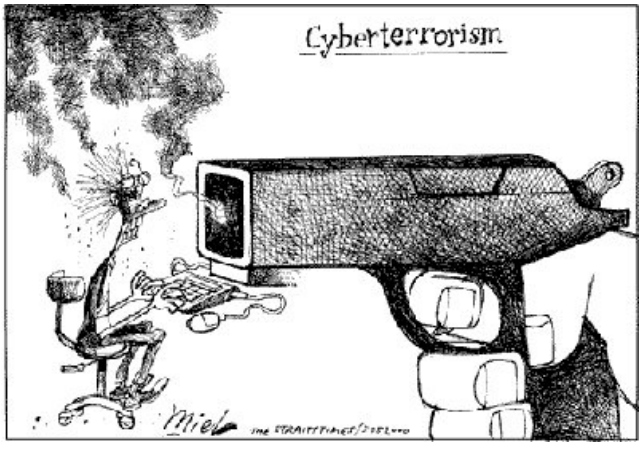
Campaigns of Cyber Aggressors
Terrorists

[continued]

In response to the terror attacks of September 11, 2001, attention to the air transportation sector of the United States and around the world grew exponentially. With the increased attention, terror attacks on this sector of American CIKR became much more difficult. Though there are cyber vulnerabilities in aircraft themselves, many physical and procedural safeguards exist that, although they would not prevent exploitations of cyber vulnerabilities within aircraft, they would likely prevent the attack from causing mass casualties. The recent publishing of exploited vulnerabilities in Aircraft Communications Addressing and Reporting System (ACARS) air traffic communications system by Hugo Tesco suggest that a cyber attack on such systems could produce a terror attack of great efficiency. However, Tesco attacked only a publicly available simulation version of ACARS software; so it remains questionable that ACARS attacks could produce an effect worth the effort.

Due to the extreme risk of these tankers and the exclusion zone policy put in place, It is possible to manipulate these tankers into traveling into areas restricted to them through GPS spoofing. It would also be possible to keep tankers in restricted areas for extended periods of time through communications jamming. The effects of this would be economic in nature. By moving these tankers closer to shore, policies in place should cause a complete and total shut down of the port and depending on the perceived intent of the tanker, an evacuation. (33)

In response to the terror attacks of September 11, 2001, attention to the air transportation sector of the United States and around the world grew exponentially. With the increased attention, terror attacks on this sector of American CIKR became much more difficult. Though there are cyber vulnerabilities in aircraft themselves, many physical and procedural safeguards exist that, although they would not prevent exploitations of cyber vulnerabilities within aircraft, they would likely prevent the attack from causing mass casualties. (38) The recent publishing of exploited vulnerabilities in Aircraft Communications Addressing and Reporting System (ACARS) air traffic communications system by Hugo Tesco suggest that a cyber attack on such systems could produce a terror attack of great efficiency. However, Tesco attacked only a publicly available simulation version of ACARS software; so it remains questionable that ACARS attacks could produce an effect worth the effort.



(38) - Pitblado, R. M., & Woodward, J. L. (2011). Highlights Of LNG Risk Technology.Journal of Loss Prevention in the Process Industries, 24(6), 827-836.

Campaigns of Cyber Aggressors
Criminal Driven Attackers

Although the evidence for criminal attacks on the CIKR of transportation is scarce, it still merits the attention for broader strategic, operational and tactical conceptualization. (38) Moreover, knowing the criminals' *mens rea* and the fact that the opportunities for its actualization are largely expanded with the potential utilization of the cyber component, its interesting to discuss a potential scenario for criminal attack on the transportation CIKR.

From the strategic perspective, the motive driving the criminal activity cause the criminals to induce any action in the physical or the cyber domain regardless of the legal or moral justification for it. The fact that the the cyber realm frees the criminals of any physical or jurisdictional boundaries, time limitations and significant financial investments for actualization of their intentions, makes the cyber a strategically plausible domain of action. In the context of the reported criminal campaigns, the drug trafficking campaign extensively rested on the drug cargo tracking and delivery information exfiltrated from the port authorities systems. A potential extension of the this activity is possible if the GPS jamming/spoofing attacks in the maritime are also considered.(39)(40)(41) Correlating the tracking information together with the possibility for circumventing the navigation of the ships, enables the criminals to act more proactively in achieving their goals, for example, they can divert any vessel of interest carrying their drug cargo to another port, knowing that the port authorities have previously seized drug containers. This also presents the possibility of allowing ships to be hijacked by diverting a ship well off its course into territory that would not be considered safe. Such attacks could be seen in economically disadvantaged areas where piracy is high.(42)

The component which is often utilized by the criminal when attacking through the cyber domain is the human element. Through phishing attacks improperly educated users expose systems to trojan horses and other malware which can degrade and destroy the integrity of systems used in transportation opening they way for systems to be exploited.

From the operational perspective, the incident proves the fact that the criminal themselves does not need to be actually proficient and have internally developed cyber capabilities. Rather, they can engage in hiring or recruiting malicious actors to infiltrate computers that tracked and controlled the movement and location of shipping containers. The same conclusion also holds for a potential collaboration between the hacker and criminal community, leading to even more disruptive consequences in the CIKR

(38) AFP. (2013, June 17). Drug Traffickers Hacked Shipping Systems to Track Large Drug Shipments | SecurityWeek.Com. *Security Week*. Retrieved October 14, 2013, from http://www.securityweek.com/drug-traffickers-hacked-shipping-systems-track-large-drug-shipments

(39) Espiner, T. (2013).

(40) Maritime Accident. (2010).

(41) Maritime Accident. (2013).

(42) Oceans Beyond Piracy. (2011). Retrieved from http://oceansbeyondpiracy.org/sites/default/files/economic_cost_of_piracy_2011.pdf]

Campaigns of Cyber Aggressors
Criminal Driven Attackers

[continued]

of transportation. For example, criminals might find it useful to utilize any exploit revealed by the hackers not just in the maritime sector, but also in the aviation and ground transportation sector to decrease the likelihood for the uncovering of their activities and increase the respective throughput of their campaigns.(43)(44)(45)(46)(47) On the other side, the hacker community might tend to financially valorize their work by getting attractive compensations for the vulnerabilities they discovered, which the criminals are willing to pay.(47) The cyber for which exploitation can easily be adapted to the intermodal nature of the shipping, rising the chances for criminal gain of any denial of service attack, malware for data exfiltration, or communication eavesdropping and payload injection pertaining the management and control systems for the maritime, air and ground traffic. As an example, criminals can take advantage of the maritime ISAC to gather information necessary to operationalize an attack on the maritime CIKR.(48)

From the tactical perspective, both the incidents shows that criminal tactics integrate the capabilities for cyber exploitation, intelligence gathering from a publicly available information and physical mobilization for actualizing their intentions. (49) Combining various exploitation approaches, both synchronously and/or sequentially instantiated within the critical CIKR transportation infrastructure, advances the criminal operation beyond the conventional means of trafficking. For example, criminals might not just use the cyber exploitation opportunities for their actual campaign, but also to divert the attention to another incident, enabling their operations to temporary stay out of interest. Further, the problems of crime attribution and actual law enforcement across different jurisdictions in case of a cybercrime, enables criminals to operate their trafficking campaigns from physical locations proven to be safe harbors for such an activity. The number of possible combinations for criminal campaign actualization is significantly increased with the involvement of the cyber component, yielding to a probable cause to suspect that the criminals will rise as a serious cyber perpetrators to the CIKR information in the near future. Adding the fact that the transportation of counterfeit and illegal goods together with the transnational organized crime are consider as most complex and extensive criminal activities, clearly bolsters this conclusion and calls for more proactive cyber monitoring and in some cases active cyber engagement to prevent from potential negative consequences to the society in overall. (50)

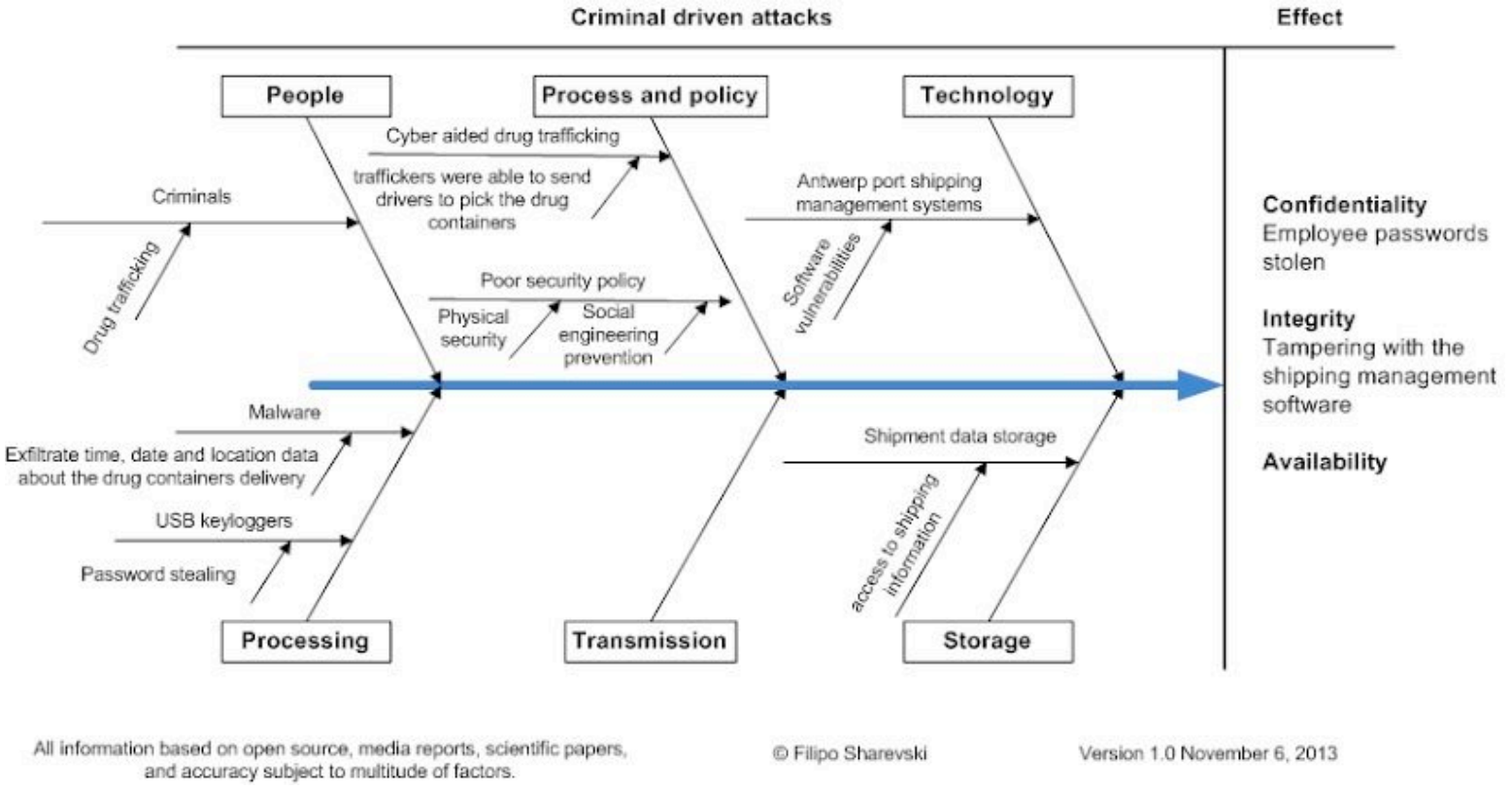
(43) Schäfer, M., Lenders, V., & Martinovic, I. (2013). Schafer, Lenders, & Martinovic, 2013
(44) Costin, A., & Francillon, A. (2012).
(45) Hoffman, D., Rezchikov, S. (2012).
(46) Teso, H. (2013).
(47) Hilkevich (2013).
(48) Internet Governance Project, 2013). Retrieved from: http://www.internetgovernance.org/2013/03/15/regulating-the-market-for-zero-day-exploits-look-to-the-demand-side/
(49) AFP. (2013).
(50) UNODC. (2013) http://www.unodc.org/unodc/en/data-and-analysis/TOC-threat-assessments.html and http://www.cbp.gov/linkhandler/cgov/trade/priority_trade/ipr/seizure/fy2012_final_stats.ctt/fy2012_final_stats.pdf]

Campaigns of Cyber Aggressors
Criminal Driven Attackers

[continued]

The Ishikawa diagram below details the effects of criminal driven attackers state on people, process, technology, processing, transmission and storage in relationship to the effects regarding confidentiality, integrity and availability in a cyber scenario.

Figure 7:



All information based on open source, media reports, scientific papers, and accuracy subject to multitude of factors.

Version 1.0 November 6, 2013

Campaigns of Cyber Aggressors
Hackers

When discussing the broad category of malicious hacking behavior, this report segments this behavior into three categories of hacking activities: hacktivistm, electronic jihad, and patriotic hacking. Framing the hacker cyber campaigns on CIKR of transportation in this classification, the research team identified hacktivistm activities and patriotic hacking. (50)(51) While the patriotic hacking is regarded as state actor activity and addressed in the previous section, no evidence suggests electronic jihad. Instead, many of the hacking activities are either attributed to teenagers or general hacking actors.(52) Further, many of the reported incidents can be identified with the black hat hacking community.(53)(54)(55)(56)(57)(58)

Although the distinct profile of the hacking perpetrators behind the cyber attacks on the CIKR of transportation considerably vary between different campaigns, an interesting aspect that merits the attention is the extensive set of tactical capabilities possessed by these cyber aggressors. The evidence for the extensive cyber exploitation capabilities used against the maritime communication systems, air traffic control systems, flight management systems and railway control, communication and dispatch systems, makes these cyber perpetrators an attractive workforce that can be employed in broader operational and strategic connotation.

Using the economic logic of supply/demand chain, the general hacker community actually as the suppliers of hacking expertise, zero-day exploits and vulnerability information, for which an increasing demand comes both from the criminals and state-actors interested in operationalized of the cyber component for their strategic intentions. Many of the exploits written by hackers can be found for sale in online forums and marketplaces. Often, these sites have been anonymized through the use of Tor network and other technologies so that participants remain protected.

From the perspective of criminals, the potential mutual collaboration between these two groups has been identified in the previous subsection, emphasizing the fact that criminals are eager to employ the hacking advances for their campaigns.(59) In a similar vein, the state actors are interested not just in simply using the hacking expertise or the zero-day vulnerabilities, but moreover to employ the hacking workforce both for military and economic espionage purposes. (60) These reports show that zero-day exploits have been driven from a case by case tactical implementation developed by hackers to an overarching strategy that nation states use to advance policy.

(50) Denning, D. E. (2003). Information technology security. In M. Brown (Ed.), Grave New World: Global Dangers in 21st Century (Vol. 24, pp. 1–12). Washington D.C.: Georgetown University Press.
(51) Murphy, D. (2011). Anonymous Attacks San Francisco BART, Leaks Site's User Data. PCMag. Retrieved October 13, 2013, from http://www.pcmag.com/article2/0,2817,2391066,00.asp
(52) Peterson. (2011).
(53) Leyden, J. (2008, January 11). Polish teen derails tram after hacking train network. Retrieved October 14, 2013, from http://www.theregister.co.uk/2008/01/11/tram_hack/
(54) Schäfer, M., Lenders, V., & Martinovic, I. (2013).
(55) Costin, A., & Francillon, A. (2012).
(56) Hoffman, D., Rezchikov, S. (2012).
(57) Teso, H. (2013). Aircraft Hacking. In *Practical Aero Series*. Retrieved from http://conference.hitb.org/hitbsecconf2013ams/hugo-teso/
(58) Guarnieri, C. (2013).
(59) Holt, T. J., & Schell, B. H. (Eds.). (2010). *Corporate Hacking and Technology-Driven Crime: Social Dynamics and Implications*. IGI Global. Retrieved from http://services.igi-global.com/resolvedoi/resolve.aspx?doi=10.4018/978-1-61692-805-6
(60) AFP. (2013)

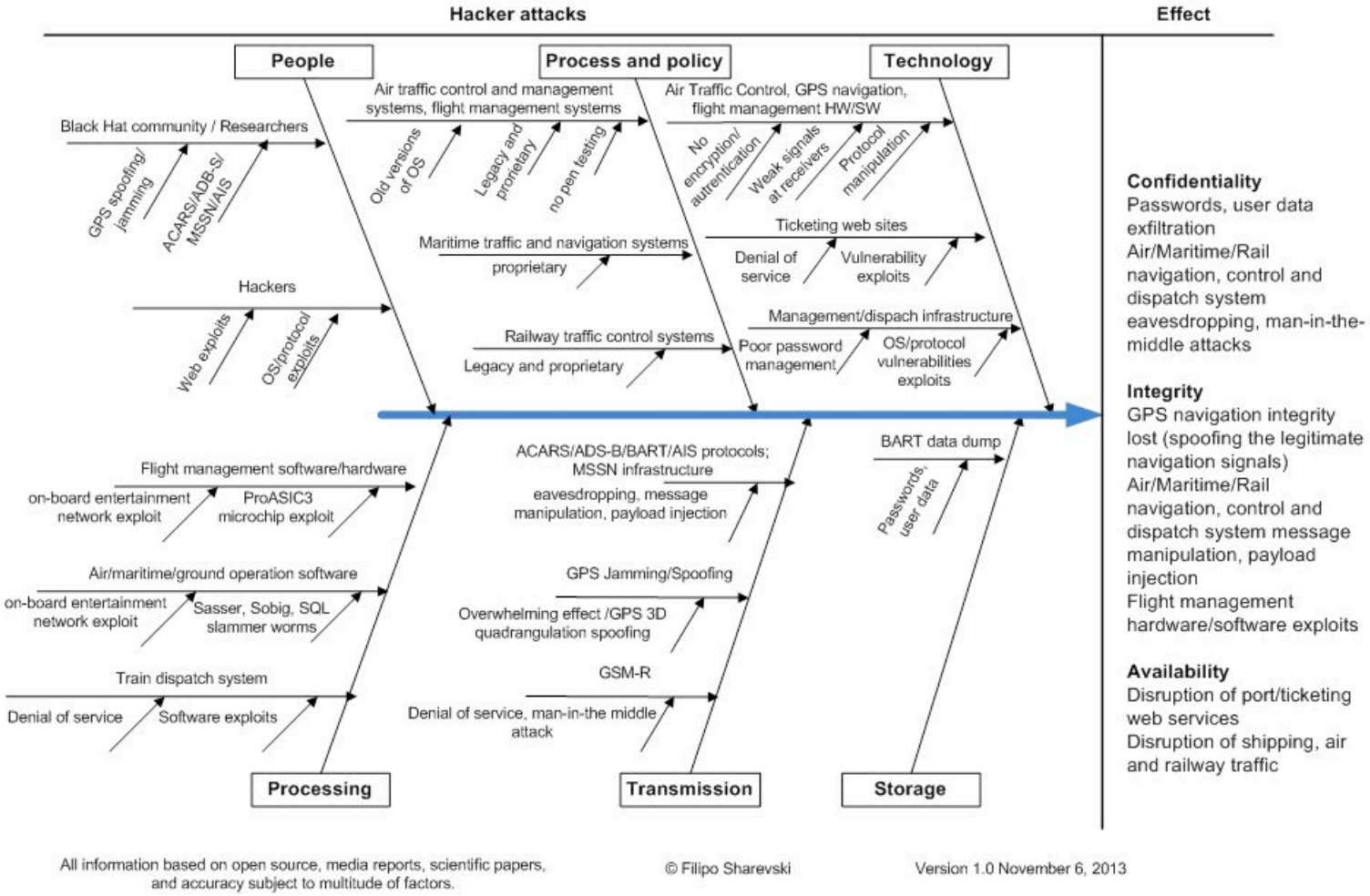
Campaigns of Cyber Aggressors
Hackers

[continued]

Despite the fact that the hacking incidents are isolated events that cannot be correlated in a broader context of synchronized, command and control guided cyber campaign against the CIKR of transportation, a future actualization of these cyber exploitations is possible in the realms of cyber warfare, cyber espionage, or criminal trafficking. Given the premise that the actual cyber exploitation supply/demand chain is an attractive concept that gains attention among this actors, this conclusion points to the fact that hacking activities take a large part in the overall cyber threat to the CIKR of transportation.

The Ishikawa diagram below details the effects of attacks from hackers (individuals and organized groups) on people, process, technology, processing, transmission and storage in relationship to the effects regarding confidentiality, integrity and availability in a cyber attack scenario.

Figure 8:



CONCLUSION

"Security is mostly a superstition. It does not exist in nature, nor do the children of men as a whole experience it. Avoiding danger is no safer in the long run than outright exposure. Life is either a daring adventure, or nothing."

Helen Keller

The enormous size and critical importance of the shipping and transportation industry to the world economy cannot be underestimated. Essential to keeping the world connected, a disruption to any of the key infrastructures embedded in this system anywhere in the world could have extensive impacts far reaching beyond the initial point of attack.

In recent years due to technologies steep evolution, ever more capable information systems have revolutionized the industry, providing great benefit to the industry, and by extension, to the world economy as a whole. These same technological advancements that have brought so much benefit also provide opportunities for catastrophic failure via the cyber domain. Based on the research documented in this report, cyber incidents impacting key shipping and transportation infrastructures and supporting systems are on the rise. New vulnerabilities created by technology are being discovered regularly. These vulnerabilities represent a large exposure to the national security of the United States that requires immediate action.

Despite a lack of large and visible incidents to date involving key shipping and transportation infrastructure in the United States, analysis of previous cyber incidents within this industry around the world show an alarming trend upward. The threat actors presented in this report are all of great concern as their capabilities are increasing and the ease of entry into these critical infrastructures and surrounding systems. Though criminals actively use the system for illicit activities; it is also likely that foreign governments have quietly penetrated key shipping and transportation control systems within the United States, or will do so in the near future, in an effort to distract the United States from offensive operations against an enemy government.

There is no doubt on this research team that this industry is extremely attractive to malicious terror groups because of the size of the sector, and because cyber attacks on key systems can be combined with kinetic means for large scale loss of life, destruction of property and economic hardships. Though the task is enormous, the United States must place stronger focus on securing its shipping and transportation infrastructure or it risks a devastating attack from any of several groups acting against the national interests of the United States.

APPENDIX A
Ground Transportation

Year	Attacker Profile	Title	Attacker Motive	Attack Vectors	Target Profile	Target Vulernabiltiy	Attack Consequences	Event
August 2003	General	Sobig Worm	Unknown	Software Vulnerability, Denial of Service	Train Dispatch and Control System	Email	Denial of e-mail service caused by massive message load.	Sobig worm affects CSX HQ, downs amtrak for 6 hours
January 2008	Hackers	Polish Train Derailment	Prank	Signals Interference	Train Dispatch Systems	Simple and unprotected communication, legacy system	12 injured, 4 trains derailed	Polish teen derails tram after hacking train network.
June 2009	General	DC Metro Train	Terrorist, Nation State	traffic management software explotation	Train Systems	Legacy systems	80 people injured	Washington DC Metro Train hits another, 80 injured
August 2011	Hackers	Anonymous hacks BART	Protest	DDoS	Web page defacement	Website vulnerability	ART's online services including web, mobile web, email and SMS unavailable on Sunday, August 14 from noon to 6.p.m.	Anonymous hacks BART websites, gains police officer PI
December 2011	General	Hackers infiltrate computers at Northwest rail company	Unknown	Denial of Service	Dispatch Systems	Unsecured SCADA controls	15 minute service delay	Computer hackers, possibly from overseas, infiltrated computer networks at Northwest rail company. The first infiltration caused schedule delays of 15 minutes. The second attack later in the day had no such effect
December 2011	General	Hacking Threat to Train Network	General CIKR cyber perpetrator motives (Amoroso, 2011, p. 6)	Denial-of-service, man-in-the middle attack	Railway communication system	GSM-R encryption keys vulnerabilities, GSM-R authentication and over the air communication	Service disruption, destruction and kinetic damage	Train switching systems, which enable trains to be guided from one track to another at a railway junction, have historically been separate from the online world. GSM-R means they will be connected to the internet, however, raising the risk from Denial of Service attacks The encryption keys are needed for securing the communication between trains and switching systems. They are downloaded to physical media like USB sticks and then sent around for installing - raising the risk of them ending up in the wrong hands.
September 2013	General	Unmanned Chicago Elevated Train accident	Unknown	traffic management software explotation	Mass transit operating equipment and passengers	CTA operational control devices	More than thirty passengers injured and taken to area hospitals.	An out of service, and apparently unmanned Chicago Transit Authority elevated train passed through several track switches and accelerated to 20 mph before ramming another CTA elevated train full of passengers, injuring more than 30 people.
September 2013	Hackers	Swedish Rail Operator SJ's website hacked	Prank	Ticketing web services	Ticket Purchasing Service	Network traffic control systems	Passengers unable to use purchasing systems	A group of Swedish teens hacked the website of rail transport operator SJ. The teens produced a denial of service attack left customers unable to purchase tickets.
September 2013	State Actor	Human implants, drones and traffic systems could all be hacked in future, Europol warns	General	Medical Equipment and Traffic Signals	Anything which would result in mass destruction, claiming the lives of civilians	Signal Jamming, Interference and Spoofing	Crippling a nation, Declaration of war	This is a warning issued by Europol. It predicted that technology could advance to such an extent by 2020 that the difference between cybercrime and physical harm will become blurred.

APPENDIX A
Ground Transportation

Year	Attacker Profile	Title	Attacker Motive	Attack Vectors	Target Profile	Target Vulernabiltiy	Attack Consequences	Event
August 2003	General	Sobig Worm	Unknown	Software Vulnerability, Denial of Service	Train Dispatch and Control System	Email	Denial of e-mail service caused by massive message load.	Sobig worm affects CSX HQ, downs amtrak for 6 hours
January 2008	Hackers	Polish Train Derailment	Prank	Signals Interference	Train Dispatch Systems	Simple and unprotected communication, legacy system	12 injured, 4 trains derailed	Polish teen derails tram after hacking train network.
June 2009	General	DC Metro Train	Terrorist, Nation State	traffic management software explotation	Train Systems	Legacy systems	80 people injured	Washington DC Metro Train hits another, 80 injured
August 2011	Hackers	Anonymous hacks BART	Protest	DDoS	Web page defacement	Website vulnerability	ART's online services including web, mobile web, email and SMS unavailable on Sunday, August 14 from noon to 6.p.m.	Anonymous hacks BART websites, gains police officer PI
December 2011	General	Hackers infiltrate computers at Northwest rail company	Unknown	Denial of Service	Dispatch Systems	Unsecured SCADA controls	15 minute service delay	Computer hackers, possibly from overseas, infiltrated computer networks at Northwest rail company. The first infiltration caused schedule delays of 15 minutes. The second attack later in the day had no such effect
December 2011	General	Hacking Threat to Train Network	General CIKR cyber perpetrator motives (Amoroso, 2011, p. 6)	Denial-of-service, man-in-the middle attack	Railway communication system	GSM-R encryption keys vulnerabilities, GSM-R authentication and over the air communication	Service disruption, destruction and kinetic damage	Train switching systems, which enable trains to be guided from one track to another at a railway junction, have historically been separate from the online world. GSM-R means they will be connected to the internet, however, raising the risk from Denial of Service attacks The encryption keys are needed for securing the communication between trains and switching systems. They are downloaded to physical media like USB sticks and then sent around for installing - raising the risk of them ending up in the wrong hands.
September 2013	General	Unmanned Chicago Elevated Train accident	Unknown	traffic management software explotation	Mass transit operating equipment and passengers	CTA operational control devices	More than thirty passengers injured and taken to area hospitals.	An out of service, and apparently unmanned Chicago Transit Authority elevated train passed through several track switches and accelerated to 20 mph before ramming another CTA elevated train full of passengers, injuring more than 30 people.
September 2013	Hackers	Swedish Rail Operator SJ's website hacked	Prank	Ticketing web services	Ticket Purchasing Service	Network traffic control systems	Passengers unable to use purchasing systems	A group of Swedish teens hacked the website of rail transport operator SJ. The teens produced a denial of service attack left customers unable to purchase tickets.
September 2013	State Actor	Human implants, drones and traffic systems could all be hacked in future, Europol warns	General	Medical Equipment and Traffic Signals	Anything which would result in mass destruction, claiming the lives of civilians	Signal Jamming, Interference and Spoofing	Crippling a nation, Declaration of war	This is a warning issued by Europol. It predicted that technology could advance to such an extent by 2020 that the difference between cybercrime and physical harm will become blurred.

Year	Attacker Profile	Title	Attacker Motive	Attack Vectors	Target Profile	Target Vulernabiltiy	Attack Consequences	Event
August 2003	General	Sobig Worm	Unknown	Software Vulnerability, Denial of Service	Train Dispatch and Control System	Email	Denial of e-mail service caused by massive message load.	Sobig worm affects CSX HQ, downs amtrak for 6 hours
January 2008	Hackers	Polish Train Derailment	Prank	Signals Interference	Train Dispatch Systems	Simple and unprotected communication, legacy system	12 injured, 4 trains derailed	Polish teen derails tram after hacking train network.
June 2009	General	DC Metro Train	Terrorist, Nation State	traffic management software explotation	Train Systems	Legacy systems	80 people injured	Washington DC Metro Train hits another, 80 injured
August 2011	Hackers	Anonymous hacks BART	Protest	DDoS	Web page defacement	Website vulnerability	ART's online services including web, mobile web, email and SMS unavailable on Sunday, August 14 from noon to 6.p.m.	Anonymous hacks BART websites, gains police officer PI
December 2011	General	Hackers infiltrate computers at Northwest rail company	Unknown	Denial of Service	Dispatch Systems	Unsecured SCADA controls	15 minute service delay	Computer hackers, possibly from overseas, infiltrated computer networks at Northwest rail company. The first infiltration caused schedule delays of 15 minutes. The second attack later in the day had no such effect
December 2011	General	Hacking Threat to Train Network	General CIKR cyber perpetrator motives (Amoroso, 2011, p. 6)	Denial-of-service, man-in-the middle attack	Railway communication system	GSM-R encryption keys vulnerabilities, GSM-R authentication and over the air communication	Service disruption, destruction and kinetic damage	Train switching systems, which enable trains to be guided from one track to another at a railway junction, have historically been separate from the online world. GSM-R means they will be connected to the internet, however, raising the risk from Denial of Service attacks The encryption keys are needed for securing the communication between trains and switching systems. They are downloaded to physical media like USB sticks and then sent around for installing - raising the risk of them ending up in the wrong hands.
September 2013	General	Unmanned Chicago Elevated Train accident	Unknown	traffic management software explotation	Mass transit operating equipment and passengers	CTA operational control devices	More than thirty passengers injured and taken to area hospitals.	An out of service, and apparently unmanned Chicago Transit Authority elevated train passed through several track switches and accelerated to 20 mph before ramming another CTA elevated train full of passengers, injuring more than 30 people.
September 2013	Hackers	Swedish Rail Operator SJ's website hacked	Prank	Ticketing web services	Ticket Purchasing Service	Network traffic control systems	Passengers unable to use purchasing systems	A group of Swedish teens hacked the website of rail transport operator SJ. The teens produced a denial of service attack left customers unable to purchase tickets.
September 2013	State Actor	Human implants, drones and traffic systems could all be hacked in future, Europol warns	General	Medical Equipment and Traffic Signals	Anything which would result in mass destruction, claiming the lives of civilians	Signal Jamming, Interference and Spoofing	Crippling a nation, Declaration of war	This is a warning issued by Europol. It predicted that technology could advance to such an extent by 2020 that the difference between cybercrime and physical harm will become blurred.

APPENDIX C
Maritime

Year	Attacker	Title	Attacker	Attack Vectors	Target Profile	Target	Attack	Event
September 2001	Hackers	Port of Houston	Disruption of port's web service Disruption of shipping	DDoS	Houston Port Authority Systems Arriving transporter ships	DDoS Vulnerability Exploitation	It froze the port's web service, which contained vital data for shipping, mooring	Aaron Caffrey, 19, was accused of crashing systems at the port of Houston in Texas by hacking into its computer systems.
December 2009	General	GPS jamming and spoofing attacks	Experimentation (proof of concept)	GPS jamming	Maritime navigation systems (GPS part of AIS)	GPS signals are susceptible to jamming, interference and	Vessel miss-navigation, sunk, hijack/ hiding vessel	GPS jamming and spoofing attacks on vessel navigation systems / experiment performed by the UK's Ministry of Defense on the THV Galatea
August 2010	State Actor	GPS Jamming Affects Ship Navigation off Korean Coast	service disruption, cyber intelligence,	GPS Jamming	GPS in ships	GPS signals are susceptible to jamming, interference and	vessel miss-navigation, sunk, hijack/ hiding vessel	GPS Jamming Affects Ship Navigation off Korean Coast
December 2010	General	GPS Jamming Research	Research	GPS Jamming	GPS in Maritime	GPS signals are susceptible to jamming, interference and spoofing	Vessel miss-navigation, sunk, hijack/ hiding vessel presence	GPS Jamming and its impact on maritime safety (Research paper, optional) http://www.porttechnology.org/images/uploads/technical_papers/PT46-09.pdf
March 2012	Criminals	Drug Traffickers	Smuggle drugs to Austalian ports (Ship, locate, retrieve) Economic Damage,	Malware, Remote Access control	Australian Customs and Border Protection Integrated Cargo System	software vulnerabilities leaving the possiblity for tracking the cargo throug the	Tracking computer terminals through malware installed to gain	Crime syndicates are exploiting flaws in a federal government computer system that have enabled them to learn if shipping containers holding their drugs are being scanned and searched by authorities.
February 2012	General	English Channel	Experimentation (proof of concept)	GPS Jamming	Maritime navigation systems (GPS part of AIS)	GPS signals are susceptable to jamming, interference and	Vessel miss-navigation, sunk, hijack/ hiding vessel	GPS Hacking May Sink Ships/GPS Hackers Put Shipping In A Jam
June 2012	State Actor	China vs India	Intelligence	systems bugs exploitation (unknown)	Naval Submarine System	systems bugs (unknown)	Data exfiltration	Chinese hackers penetrated the computers at Indian Eastern Naval Command - china vs india
April 2013	Hackers	Automatic Identification System (AIS) attack	General CIKR	hijack AIS traffic, eavesdropping on AIS messages,	Maritime Identification and Navigation System	Automatic Identification System (AIS) lack of encryption and	collisions at sea, hijacking/hiding a vessel, miss-navigation	HD's serial port server research highlights the inherent insecurity of a large amount of network-enabling devices that bridge to the Internet normally isolated systems such as fuel pumps, oil and gas pipelines, power grids, traffic lights and many more odd and scary things.
April 2013	General	Cyber Vulnerabilities found in Newest U.S. Combat Ship	Experimentation (proof of concept)	U.S. Navy Internal (Confidential)	U.S.S. Freedom	Classified (unknown)	Classified Research	The newest combat ship in the U.S. Navy's arsenal, the U.S.S. Freedom, was found during a fleet-wide cyber assessment by Navy cyber security experts to have major cyber security vulnerabilities. The Navy is working with its contractors to correct the deficiencies, which remain classified. The Navy plans to buy 52 such ships in coming years.
June 2013	Criminals	Drug Traffickers	Smuggle drugs to US ports (Ship, locate, retrieve) Economic Damage, Criminal	Malware, Remote Access control	Navigation and Surveilence Systems (Antwerp city)	Malware infection, remote access vulnerability Navigation and Surveillance Systems	Tracking computer terminals through malware installed to gain access.	Drug Traffickers Hacked Shipping Systems to Intercept Large Drug Shipments

REFERENCES

Aero News Network. (2010). FAA Tells Boeing To “Hack Proof” 747-8, -8F. Retrieved October 12, 2013, from http://www.aero-news.net/index.cfm?do=main.textpost&id=c54094a8-d6cd-404f-82d6-5598267eea23

AFP. (2013, June 17). Drug Traffickers Hacked Shipping Systems to Track Large Drug Shipments | SecurityWeek.Com. *Security Week*. Retrieved October 14, 2013, from http://www.securityweek.com/drug-traffickers-hacked-shipping-systems-track-large-drug-shipments

Akamai. (2013). *The State of the Internet*.

Anstee, D. (2013, October 16). Q3 findings from ATLAS - Arbor Networks. Retrieved November 24, 2013, from http://www.arbornetworks.com/corporate/blog/5025-q3-findings-from-atlas

Blasco, J. (2013, October 16). OTX Snapshot: Top Malware Detected | AlienVault. Retrieved November 24, 2013, from http://www.alienvault.com/open-threat-exchange/blog/otx-snapshot-top-malware-detected

Bureau of Transportation Statistics. (2009). *Transportation Commodity Flow Survey*. Retrieved from http://www.rita.dot.gov/bts/sites/rita.dot.gov.bts/files/publications/pocket_guide_to_transportation/2012/html/table_04_06.html

Bowden, A., & Basnet, S. (2012). The economic cost of Somali piracy 2011. *One Earth Future Foundation, Louisville, CT, February*.

Costin, A., & Francillon, A. (2012). Ghost in the Air (Traffic): On insecurity of ADS-B protocol and practical attacks on ADS-B devices. *Black Hat USA*. Retrieved from https://www.eurecom.fr/fr/publication/3788/download/rs-publi-3788.pdf

De Lama, G., & McNulty, T. (1991, January 24). Bush Says Desert Storm `On Schedule`. *Chicago Tribune*. Retrieved November 19, 2013, from http://articles.chicagotribune.com/1991-01-24/news/9101070715_1_cheney-and-powell-gen-colin-powell-pentagon

Denning, D. E. (2003). Information technology security. In M. Brown (Ed.), Grave New World: Global Dangers in 21st Century (Vol. 24, pp. 1–12). Washington D.C.: Georgetown University Press.

Espiner, T. (2013). THV Galatea trial. ZDNet Security. Retrieved October 11, 2013, from http://www.zdnet.com/uk-sentinel-study-reveals- gps-jammer- use-3040095106/

Falliere, N., Murchu, L. O., & Chien, E. (2011). W32. stuxnet dossier. *White paper, Symantec Corp., Security Response*. Retrieved from http://www.h4ckr.us/library/Documents/ICS_Events/Stuxnet%20Dossier%20(Symantec)%20v1.4.pdf

Fire triangle. (2013, November 7). In *Wikipedia, the free encyclopedia*. Retrieved from http://en.wikipedia.org/w/index.php?title=Fire_triangle&oldid=580616932

REFERENCES

Fogarthy, K. (2011). Is it really possible to hack a 747's engines in-flight? IT World. Retrieved October 12, 2013, from http://www.itworld.com/security/223843/it-really-possible-hack-747s-engines

GPS Hackers Put Shipping In A Jam» Maritime Accident Casebook. (2012, February 23). *Maritime Accident Casebook*. Retrieved October 14, 2013, from http://maritimeaccident.org/2012/02/gps-hackers-put-shipping-in-a-jam/

GPS Hacking May Sink Ships» Maritime Accident Casebook. (2010, February 23). *Maritime Accident Casebook*. Retrieved October 14, 2013, from http://maritimeaccident.org/2010/02/gps-hacking-may-sink-ships/

Guarnieri, C. (2013). Spying on the Seven Seas with AIS. Information Security. Retrieved November 10, 2013, from https://community.rapid7.com/com munity/infosec/blog/2013/04/29/spying-on-the-seven-seas-with-ais

Hacking "threat to train network." (2011, December 29). *Telegraph.co.uk*. Retrieved from http://www.telegraph.co.uk/technology/news/8982404/Hacking-threat-to-train-network.html

Hightower, M., Gritzo, L., Ragland, D., Luketa-Hanlin, A., Covan, J., Tieszen, S., et al. (2004). Guidance on Risk Analysis and Safety Implications of a Large Liquefied Natural Gas (LNG) Spill Over Water. Sandia National Laboratories,SAND2004(6258). Retrieved October 15, 2013, from http://www.osti.gov/scitech/biblio/882343

Handbook: US Army FMI Open Source Intelligence. (2008). Retrieved from http://www.fas.org/irp/doddir/army/fmi2-22-9.pdf

Hoffman, D., Rezchikov, S. (2012). Busting the BARR: Tracking "Untrackable" Private Aircraft for Fun & Profit. DEFCON 20.

Holt, T. J., & Schell, B. H. (Eds.). (2010). *Corporate Hacking and Technology-Driven Crime: Social Dynamics and Implications*. IGI Global. Retrieved from http://services.igi-global.com/resolvedoi/resolve.aspx?doi=10.4018/978-1-61692-805-6

How to Hack Into a Boeing 787. (2008, February 20). *FoxNews.com*. Text.Article. Retrieved October 14, 2013, from http://www.foxnews.com/story/2008/02/20/how-to-hack-into-boeing-787

Information about the Fire Triangle/Tetrahedron and Combustion. (2011). *Safelincs Ltd.* Retrieved November 19, 2013, from http://www.firesafe.org.uk/information-about-the-fire-triangletetrahedron-and-combustion/

Internet Governance Project, 2013). Retrieved from: http://www.internetgovernance.org/2013/03/15/regulating-the-market-for-zero-day-exploits-look-to-the-demand-side/

King, L. C. (2011). Quality Control Review on the Vulnerability Assessment of FAA's Operational Air Traffic Control System. Retrieved from http://trid.trb.org/view.aspx?id=1104102

REFERENCES

Leyden, J. (2008, January 11). Polish teen derails tram after hacking train network. Retrieved October 14, 2013, from http://www.theregister.co.uk/2008/01/11/tram_hack/

Lowe, M. (2012). Chinese hackers penetrate Navy's computer. Maritime Security Review. Retrieved November 10, 2013, from http://www.marsecreview.com/2012/07/intrusion-episode/

Maritime Accident. (2010). GPS Hacking May Sink Ships. Retrieved October 11, 2013, from http://maritimeaccident.org/2010/02/gps- hacking- may-sink-ships/

Maritime Accident. (2013). GPS Hackers Put Shipping In A Jam. Retrieved October 11, 2013, from http://maritimeaccident.org/2012/02/gps-hackers-put-shipping-in-a-jam/

Maritime Security Council. (2013). *Maritime ISAC*. Retrieved from http://www.maritimesecurity.org/index.html

National Transportation Safety Board. (2010). NTSB CITES TRACK CIRCUIT FAILURE AND MATA'S LACK OF A SAFETY CULTURE IN 2009 FATAL COLLISION. Press Release. Retrieved October 13, 2013, from http://www.ntsb.gov/news/2010/100727c.html

Oceans Beyond Piracy. (2011). Retrieved from http://oceansbeyondpiracy.org/sites/default/files/economic_cost_of_piracy_2011.pdf

Panja, B., Bhargava, B., Pati, S., Paul, D., Lilien, L. T., & Meharia, P. (n.d.). Monitoring and Managing Cloud Computing Security using Denial of Service Bandwidth Allowance. Retrieved from http://www.cs.purdue.edu/homes/bb/monitoring-cloud-security.pdf

Peterson, S. (2011). Iran hijacked US drone, says Iranian engineer. The Christian Science Monitor. Retrieved October 12, 2013, from http://www.csmonitor.com/World/Middle-East/2011/1215/Exclusive-Iran-hijacked-US-drone-says-Iranian-engineer-Video

Pitblado, R. M., & Woodward, J. L. (2011). Highlights Of LNG Risk Technology.Journal of Loss Prevention in the Process Industries, 24(6), 827-836.

Press Release [July 27, 2010] - NTSB - National Transportation Safety Board. (2010, July 27). *National Transportation Safety Board*. Retrieved October 14, 2013, from http://www.ntsb.gov/news/2010/100727c.html

Regulating the Market for Zero-day Exploits: Look to the demand side | IGP Blog. (2013, March 15). Retrieved November 25, 2013, Retrieved from http://www.internetgovernance.org/2013/03/15/regulating-the-market-for-zero-day-exploits-look-to-the-demand-side/

REFERENCES

Schäfer, M., Lenders, V., & Martinovic, I. (2013). Experimental analysis of attacks on next generation air traffic communication. In *Applied Cryptography and Network Security* (pp. 253–271). Retrieved from http://link.springer.com/chapter/10.1007/978-3-642-38980-1_16

Storm, D. (2012a). Curious hackers inject ghost airplanes into radar, track celebrities' flights. Computer World. Retrieved October 12, 2013, from http://blogs.computerworld.com/cybercrime-and- hacking/20775/curious- hackers- inject- ghost-airplanes-radar-track-celebrities- flights

Storm, D. (2012b). Civilian drones vulnerable to hackers, can be hijacked, used as missiles. Computer World. Retrieved October 12, 2013, from http://blogs.computerworld.com/security/20593/civilian-drones- vulnerable- hackers-can-be- hijacked-used-missiles

Storm, D. (2013). Hacker uses an Android to remotely attack and hijack an airplane. Computer World. Retrieved October 12, 2013, from http://blogs.computerworld.com/cybercrime-and- hacking/22036/hacker- uses-android-remotely-attack-and-hijack-airplane

Strohmeier, M., Lenders, V., & Martinovic, I. (2013). Security of ADS-B: State of the Art and Beyond. *arXiv preprint arXiv:1307.3664*. Retrieved from http://arxiv.org/abs/1307.3664

Sun, L. H., & Glod, M. (2009, June 23). At Least 6 Killed in Red Line Crash. *The Washington Post*. Retrieved from http://www.washingtonpost.com/wp-dyn/content/article/2009/06/22/AR2009062202508.html

Sutton's law. (2013, May 30). In *Wikipedia, the free encyclopedia*. Retrieved from http://en.wikipedia.org/w/index.php?title=Sutton%27s_law&oldid=557575615

Teso, H. (2013). Aircraft Hacking. In *Practical Aero Series*. Retrieved from http://conference.hitb.org/hitbsecconf2013ams/hugo-teso/

UNODC. (2013). Retrieved from http://www.cbp.gov/linkhandler/cgov/trade/priority_trade/ipr/seizure/fy2012_final_stats.ctt/fy2012_final_stats.pdf]

Willie Sutton. (2013, November 11). In *Wikipedia, the free encyclopedia*. Retrieved from http://en.wikipedia.org/w/index.php?title=Willie_Sutton&oldid=581243459

Storm, D. (2012a). Curious hackers inject ghost airplanes into radar, track celebrities' flights. Computer World. Retrieved October 12, 2013, from http://blogs.computerworld.com/cybercrime-and- hacking/20775/curious- hackers- inject- ghost-airplanes-radar-track-celebrities- flights

REFERENCES

Storm, D. (2012b). Civilian drones vulnerable to hackers, can be hijacked, used as missiles. Computer World. Retrieved October 12, 2013, from http://blogs.computerworld.com/security/20593/civilian-drones- vulnerable- hackers-can-be- hijacked-used-missiles

Storm, D. (2013). Hacker uses an Android to remotely attack and hijack an airplane. Computer World. Retrieved October 12, 2013, from http://blogs.computerworld.com/cybercrime-and- hacking/22036/hacker- uses-android-remotely-attack-and-hijack-airplane

Strohmeier, M., Lenders, V., & Martinovic, I. (2013). Security of ADS-B: State of the Art and Beyond. *arXiv preprint arXiv:1307.3664*. Retrieved from http://arxiv.org/abs/1307.3664

Sun, L. H., & Glod, M. (2009, June 23). At Least 6 Killed in Red Line Crash. *The Washington Post*. Retrieved from http://www.washingtonpost.com/wp-dyn/content/article/2009/06/22/AR2009062202508.html

Sutton's law. (2013, May 30). In *Wikipedia, the free encyclopedia*. Retrieved from http://en.wikipedia.org/w/index.php?title=Sutton%27s_law&oldid=557575615

Teso, H. (2013). Aircraft Hacking. In *Practical Aero Series*. Retrieved from http://conference.hitb.org/hitbsecconf2013ams/hugo-teso/

UNODC. (2013). Retrieved from http://www.cbp.gov/linkhandler/cgov/trade/priority_trade/ipr/seizure/fy2012_final_stats.ctt/fy2012_final_stats.pdf]

Willie Sutton. (2013, November 11). In *Wikipedia, the free encyclopedia*. Retrieved from http://en.wikipedia.org/w/index.php?title=Willie_Sutton&oldid=581243459

AUTHORS [in alphabetical order]

Faisel Al-Askandrani
Faisal Talal Al-Askandrani was born in Khobar, Saudi Arabia in 1984. In 2002, he received a full scholarship from Saudi Aramco to pursue his undergrad education. In 2008, he earned his undergraduate degree from the University of New Branswick, Canada. Al-Askandrani received a Bachelor of Computer science majoring in Information System and a Minor in Business Administration. During his undergraduate degree he was hired by the university as a Java Tutor.

Upon graduation, Al-Askandrani started working in Saudi Aramco, Dhahran for one year in the Oil Company's Central Database for Real-Time Data under the Reservoir Description & Simulation Department. In 2010, Al-Askandrani was deployed to the field for two years in Khurais Producing Department as Process Control Network Engineer, and Real-Time Data specialist. By the end of his deployment, Al-Askandrani was able to acquire the Cisco Certified Network Associate and Certified Wireless Network Administrator. After his deployment, he was positioned in the Companies Headquarters in the Process Control Service department in which he reviewed network, security standards, and reviewed projects compliance in those fields. Al-Askandrani co-authored a study under the name “Intelligent Field Converged IP Network for Semi-Real Hydrocarbon Process Automation Applications (HPAA) Case Study,” that was presented in December 18-22, 2010 at the IEEE International Energy Conference, Manama, Bahrain.

Due to his outstanding efforts in the Shamoon malware Cyber-attack that targeted the company’s operations. Al-Askandrani was awarded a Full scholarship to pursue his master’s degree in Cyber Security and Forensic. Currently, Al-Askandrani is a grad student in Cyber forensic at Purdue University. His main research focus is in the areas of security and networking, risks, mitigations, strategic infrastructure development, policy making in relation to the Supervisory Control, And Data Acquisition Systems (SCADA) with the world wide convergence of networks trend.

Eric Amos
Donald Eric Amos was born in 1968 in Indianapolis, Indiana. He received his BSEE from Purdue University in 1994. After attending Officer Candidate School in Pensacola, Florida he received a commission as an Ensign in the United States Navy in 1995. His first duty was 1st Division Officer on USS Independence CV-62 in Yokosuka, Japan. He was then assigned to the USS Normandy CG-60 out of Norfolk, Virginia as Main Propulsion Assistant in 1999. Rotating to shore duty he served as a Training Liaison Officer at Afloat Training Group Norfolk in 2001. He was then assigned to USS Boone FFG-28 ported in Mayport, Florida in 2002 as Combat Systems Officer. After finishing his military service he is currently pursuing his Masters Degree through the CERIAS program at Purdue University.

AUTHORS [in alphabetical order]

Joe Beckman
Joe Beckman was born in Hammond, Indiana, USA in 1976. He received his Bachelor of Science in business from Indiana University in 1998, and his MBA from Valparaiso University in 2007. Following his graduation from Indiana University, Joe worked as a software security consultant for Deloitte & Touche, and as the CIO and COO for a his family's building materials supply company. During his tenure, the company grew from $14MM to 46MM in annual revenue, and tripled its net profit percentage.

In 2013, Joe joined The Center for Education and Research in Information Assurance and Security (CERIAS) at Purdue University. He is studying for his Ph.D. in Interdisciplinary Information Security under the Scholarship for Service (SFS) CyberCorp program. His research interests include digital forensics, the economics of information security, quality systems in information assurance and security, and information security policy.

Nikhil Boreddy
Nikhil Boreddy was born in Narasaraopet, India, in 1990. He received B.E. degree in Computer Science & Engineering from the Manipal University, Manipal, India, in 2013, and is pursuing his MS in Cyber Forensics from Purdue University.

In 2010, he interned at Nettech Pvt LTD, India, a leading network security company. He was the president of Indian Society for Technical Education, Manipal University chapter from 2011 to 2012. His current research interests include digital crime investigation tools, secure hashing, file header analysis and web security. Mr. Boreddy is a life member of Indian Society for Technical Education (ISTE), India.

Brian Curnett
Brian Curnett was born in Atlanta, Georgia, in 1990. He received a B.S. in Chemistry from Purdue University in 2013. During this time he served as a task force analyst for the United States Marshals Service and as a teaching assistant in Forensic Science for Purdue University. In 2013, he joined the Center for Education and Research in Information Assurance and Security at Purdue University as part of the Interdisciplinary Information Security Masters Program. His main research focus is in the areas of intelligence analysis, decision making, Bayesian algorithms, and policy analysis. He currently a recipient of the CyberCorps Scholarship for Service Fellowship award.

AUTHORS [in alphabetical order]

Chris Martinez
Christopher Martinez was born in Silverdale, Washington, USA in 1989. He received his Bachelor of Science from The University of Washington in 2013. Prior to attending The University of Washington, he spent numerous years developing and administering command, control and intelligence (C2I) systems for the United States Navy (USN) at Naval Submarine Base Bangor.

In 2012, Christopher joined The Center for Education and Research in Information Assurance and Security (CERIAS) at Purdue University. He is studying for his Masters of Science in Interdisciplinary Information Security under the Scholarship for Service (SFS) CyberCorp program. His research interests include digital forensics, command and control (C2) policy and regulation, human-computer interaction (HCI), information warfare, and computing legislation. He is an active member of the National Eagle Scout Association (NESA), USA Freedom Corps, Upsilon Pi Epsilon, and the Association of Computing Machinery (ACM).

Kelley Misata
Kelley Misata was born in Endwell, New York, in 1968. She holds a Bachelor of Science in Marketing from Westfield University (1990) and a Masters Degree in Business Administration from Bentley University (1995). Kelley combines 15 years of professional success in strategic business development, training and consulting with a unique perspective as a survivor of cyberstalking campaign which has lasted over 5 years. Currently she is Director of Outreach, and Communications of The Tor Project and Vice President of the Open Information Security Foundation (OISF). Her work at both Tor and OISF spans across fundraising, advocacy, media management, marketing and outreach activities with a wide array of stakeholders.

In 2012, Kelley joined CERIAS, Purdue University as an active member of the PhD Interdisciplinary Program in Information Security. Studying under the direction of Dr. Eugene Spafford and Dr. Marc Rogers Kelley's research interests are draw to policy debates surrounding privacy, anonymity and freedom speech online, as well as, the use of technology in human trafficking.

AUTHORS [in alphabetical order]

Filipo Sharevski
Filipo Sharevski was born in Skopje, Republic of Macedonia, in 1985. He received the B.Eng. degree and M.Sc.Eng, degree in electrical engineering and telecommunications from the Ss. Cyril and Methodius University, Skopje, Macedonia in 2004 and 2009 respectively. In the 2003-2008 period he was a teaching assistant at the Center for Wireless and Mobile Communications, Faculty of Electrical Engineering and Information Technologies in Skopje. From 2008 to August 2012 he was a principle engineer responsible for the intelligent and packet core network in Vip Operator Macedonia – member of the Vodafone group.

In 2012, he joined CERIAS, Purdue University as part of the Interdisciplinary Ph.D. program in Information Security. His main areas of research interest include digital forensics, mobile and large-scale network forensics, mobile and wireless network security solutions, encrypted voice and data streams analysis, and next generation mobile networking solutions. He is currently working on his Ph.D. thesis in the area of mobile network forensics, with Dr. Melissa Dark as his advisor. He is a long time IEEE member, and he was received several IEEE awards, including the award for the best young researcher at the 2009 IEEE Telecommunication Forum held in Belgrade, Serbia.

Hans Vargas
Hans Vargas was born in Moyobamba, Peru, in 1981. He received his Bachelor in Systems Engineering from North University, Trujillo, Peru in 2004. He has worked for IBM Peru, consulted for Petroperu, Purdue Extension, a startup called Imaginestics at Purdue Research Park, before joining CERIAS at Purdue University in fall 2012 as part of the Interdisciplinary Masters program in Information Security. His main areas of research interest include information security policy and cloud computing. He is currently working on his Master thesis in the area of Cost-Benefit Analysis for the Indiana Cybersecurity Services Center with Dr. Melissa Dark as his advisor.