George Washington's Teachings On Cyberwar

The Military Geography of Cyberspace

Robert Zager and John Zager

George Washington called West Point, "the key to the continent."[1] Established as a military post by Washington's order of 25 January 1778, West Point is the oldest continuously occupied military post in the United States.

What can 21st Century cyber warriors learn from an 18th Century surveyor on horseback? Obviously the world of George Washington was very different from our own. Nevertheless, the reasoning that Washington employed in establishing the fortifications at West Point is instructive to modern cyber warriors.

Washington's fortifications at West Point applied the principles of military geography, the field of geography dealing with natural and manmade features that may affect the planning and conduct of military operations, to the engagement with the British. We discuss how the concepts of military geography can be applied to engagements in cyberspace. We propose that the application of the concepts of military geography requires that the cognitive dimension of the information environment be incorporated as a new fourth layer in the cyberspace model of Joint Publication 3-12(R*) Cyberspace Operations*. Finally, we discuss how the *NSA Methodology for Adversary Obstruction* provides a system to implement the principles of military geography in cyberspace.

George Washington and West Point[2]

Great commanders, past and present, understand that topography, weather, and climate not only affect strategies but battle and support plans. History in fact is replete with enormous penalties incurred by those who paid too little attention to geographic factors.

- General John W. Vessey, Jr., Chairman of the Joint Chiefs of Staff, 1982-1985[3]

The Hudson River Valley is part of a dividing line that separates the mid-Atlantic colonies from the New England colonies. This map, figure 1, is an overview of the Military Geography of the Revolutionary War.

Figure 1 illustrates the dividing line running from British Canada through Lake Champlain and its tributaries then down the Hudson River to British-held Long Island. The British and the Colonists knew that control of the Hudson River Valley would cut-off the New England colonies from the mid-Atlantic colonies, providing a significant advantage to the British forces. Controlling the routes from the Saint Lawrence River to the Hudson Valley would allow the British to cut-off agricultural products from inland New York, disrupt the logistics of the

Figure 1 - The Strategic Setting. Source: Dunwell[4]

Continental Army, and hamper trade between the New England Colonies and the Mid-Atlantic Colonies. The British needed to control this dividing line, the Continental Army needed to prevent the British from gaining this control.

Reversing a series of early defeats, on 27 January 1778, the Continental Army was able to retake the Hudson Valley Highlands. As George Washington planned the refortification of the Hudson Valley Highlands, he applied the hard won lessons of his earlier defeats. These lessons were lessons of military geography.

> Military geography … concentrates on the influence of physical and cultural environments over political-military policies, plans, programs, and combat/support operations of all types in global, regional, and local contexts. John M. Collins, *Military Geography*.[4]

As Figure 2 illustrates, layers of favorable factors (for the Continental Army) of military geography converged at West Point. Navigation of the Hudson River is obstructed by West Point and Constitution Island. A sailing vessel navigating this narrow "S" stretch of river is forced to travel slowly having to reset its sails at least three times in order to pass West Point. A fleet of sailing vessels will be subject to artillery fire as the fleet comes to a virtual standstill as each ship takes its turn navigating the "S." West Point sits high above the river, allowing artillery to target the decks of enemy vessels. Constitution Island is separated from the mainland by a marshland to the east, offering attackers little concealment and difficult land passage. Despite being an island, the marshland to the east is not navigable, providing no opportunity for naval assault of the Constitution Island from the east. The river is narrow between West Point and Constitution Island, providing an ideal opportunity to lay the Great Chain[5] to obstruct the river. West Point was difficult to attack by land, yet it offered defensible routes of communication.

Figure 2 West Point. Source: The Authors

Washington's genius in the fortifications of West Point can be seen as the application of the principles of military geography.[6] These principles can be applied to engagements in cyberspace.

The Stuff of Cyberspace

[T]he Internet is not something that you just dump something on... It's a series of tubes.

- Senator Ted Stevens (R, AK) [7]

Cyberspace does not exist in an ethereal realm separated from the physical world. Just as kinetic warfare is conducted subject to the opportunities and impediments imposed by the battlespace, so to, cyber warfare operates subject to the constraints imposed by the battlespace. By effectively exploiting the opportunities and impediments imposed by the terrain, George Washington was able to leverage a

chokepoint in the Hudson River to his advantage. Military Geography provides a framework to analyze the interaction between the adversaries against the backdrop of the battlespace.[8]

Rolf Landauer observed, "Information is inevitably inscribed in a physical medium. It is not an abstract entity…The physical nature of information ties it to all the restrictions and possibilities of our actual physical universe."[9] Consider a simple example of cyberspace – data on a USB thumbdrive. The information and the device are inextricable. Destroying the device destroys the information on it. Possessing the device affords the opportunity to access the information stored on it. When the device is plugged into a network, the information on the USB drive becomes accessible over the network and the network becomes a means for all things connected to the network to communicate with one another; correspondingly, if the network access is impaired, access to the data on the connected devices is impaired. When the device is part of a system which includes physical controllers, the information on the device can monitor connected physical sensors and issue instructions to the physical controllers. When the device is part of a system with human interfaces, people can interact with the data on the device. Within the system connected to the device, decisions are made by physical control systems and people. The relationship between the information on the device and the decision making is interactive – decisions modify the data and the data modifies decisions. Although the adversarial engagement is about the information on the thumbdrive, the military geography of that engagement is dictated by the physical environment of the thumbdrive. The destruction of Iranian centrifuges is an example of these principles. According to published reports, the Stuxnet malware was introduced into the Iranian systems when someone inserted a USB device containing Stuxnet code into a computer on a network that was connected to the industrial controllers which operated the centrifuges.[10] The environment in which the USB device operates is cyberspace. Cyberspace consists of four layers. The first three of these layers, as described in Joint Publication 3-12(R), *Cyberspace Operations*, are:[11]

1. The physical network layer comprises the physical elements of cyberspace. These physical elements are the hardware, systems software and the infrastructure that supports the network.
2. The logical network layer contains those elements of the network that are related to other, abstracted from the physical layer. JP 3-12(R) gives the example of a website that can be hosted in multiple locations but which is accessed with a single URL.
3. The cyber-persona layer is a higher level of abstraction which uses rules that apply in the logical layer to develop digital representations of user.

As the Stuxnet example shows, an important element of cyberspace occurs above the cyber-persona layer. That element is decision-making. In Stuxnet two key decisions were made:

1. A person decided to insert the thumbdrive into the uranium enrichment network; and
2. An industrial controller "decided" to overspin the centrifuges.

Using the terminology of Joint Doctrine, "The cognitive dimension encompasses the minds of those who transmit, receive, and respond to or act on information."[12] In cyberspace, decisions can be made by human beings and by non-person entities ("NPE") comprised of software and programmed devices.[13] With the delegation of decision-making to software and programmed devices, the command and control agents of cyberspace consist of human beings and NPE. We propose that the cognitive layer, populated by the minds of human beings and NPE, be added as the fourth layer of cyberspace. The revised layers

of cyberspace are shown in Figure 3.

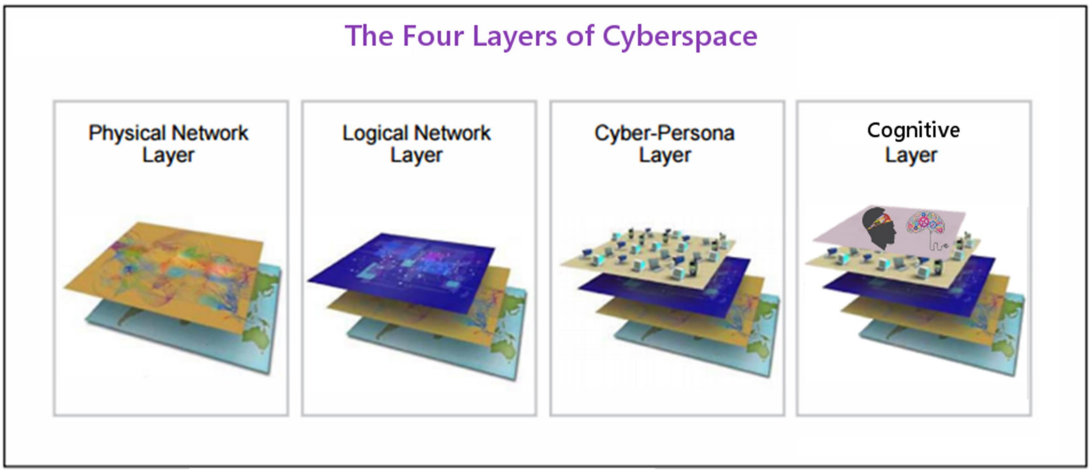


Figure 3 The Four Layers of Cyberspace. Adapted from JP 3-12(R)

With the four layers of cyberspace as a framework, the military geography of cyberspace comes into focus. Cyberspace is a communications system through which command and control is exercised. All cybersecurity compromises can be seen in the context of these communication, and command and control functions.

In 2006, Senator Stevens was widely ridiculed for his metaphor, quoted above, comparing the internet to a series of tubes. [14] And, yet, as discussed below, his observation provides an astute framework for understanding the military geography of cyberspace

Cyber Military Geography Overview

Depending on the specific characteristics of the attacks, unprecedented cascading failures of our major infrastructures could result. In that event, a regional or national recovery would be long and difficult and would seriously degrade the safety and overall viability of our Nation.

- 2004 Graham Commission Report[15]

Brig. Gen. Mark Kimmitt famously observed, "I'm an artillery officer, and I can't fire cannons at the internet."[16] And yet, seeking out the tubes of cyberspace reveals the vast opportunities and vulnerabilities of cyberspace. Seen as tubes, cyberspace presents four distinct attack surfaces:

1. The tubes themselves, the data within the tubes, and the supporting infrastructure of the tubes (the physical network layer)
2. The connections between the tubes (the logical network layer)
3. Use of the tubes (the cyber-persona layer)
4. The tube users (the cognitive layer)

Attack the Physical Network Layer. The Department of Homeland Security identifies 16 critical infrastructure sectors "that compose the assets, systems, and networks, whether physical or virtual, so vital to the United States that their incapacitation or destruction would have a debilitating effect on security, national economic security, national public health or safety, or any combination thereof."[17]

Although cyberspace is not identified as a critical sector, the Communications Section, which compromises elements of the physical network layer of cyberspace, is identified as a critical sector. The

Sector Overview of the Communications Sector discusses the interdependence of the Communications Sector, the Energy Sector, the Information Technology Sector, the Emergency Services Sector and the Transportation Systems Sector.[18] For example, the Energy Sector provides the power to run the Communications Sector and the Communications Sector provides the means to monitor and control the delivery of electricity.

A 2012 natural disaster revealed the interdependence of critical infrastructure. In June 2012, the eastern United States suffered a derecho. Unlike a hurricane, which develops slowly and offers the opportunity for planning in anticipation of the storm, derechos are windstorms that occur with little or no advance notice. The lack of advance notice and preparation time makes a derecho more like a man made disruptive event. In its January 2013 report on the 2012 derecho, the Federal Communications Commission described how the disruption of power caused by the derecho forced the cell phone system to fail over to its emergency battery power; when that emergency power was exhausted (in a matter of a few hours), the power failure ultimately led to the degradation of telecommunications network– including the degradation of large portions of the 911 system in six states. Seventeen 911 call centers in three states were lost completely, affecting more than 2 million people. [19] The FCC's report on the derecho details how the loss of power for cell phone towers cascaded from system to system, ultimately degrading the entire emergency telecommunications system for a significant portion of the nation.

Power is but one vulnerability that can take down the communication functions of cyberspace. A 2007 incident further illustrates the surprising interdependence of the elements of the physical layer of cyberspace – independencies which show how an adversary can the leverage of vulnerabilities of a one system to disrupt other systems. In 2007, San Diego, California experienced the simultaneous failure of a number of systems.[20] The civilian air traffic control system was malfunctioning. Emergency medical pagers and cell phones stopped working. The harbor's boat traffic management failed. ATM machines failed. The cell phone system failed. The disruptions lasted for about 2 hours. After three days of investigation all of these disruptions were attributed to the same source – a U.S. Navy jamming exercise interfered with the Global Navigation Satellite System (GNSS) Positioning, Navigation, Timing (PNT) timing signal.

According to DHS, 15 of the critical infrastructure sectors are dependent on the PNT timing signal; **the GPS timing signal is considered essential for 11 of the critical infrastructure sectors.**[21] There is a vast array of services that are dependent upon the weak PNT signal.[22] The PNT timing signal is used to synchronize a wide variety of networks including the communications networks, financial networks and the power grid.[23] The positioning and navigation signals are used for location and navigation. The North Koreans have deployed large PNT jamming trucks with ranges on the order of 60 miles.[24] On the other hand, small easily concealed jammers (such as battery powered hockey-puck devices or devices that plug into car cigarette lighters) with a disruptive range of 10 miles are easy to deploy, hard to find and could be distributed in substantial numbers.[25] Standard electronic warfare responses (e.g., HARM missiles) to battlefield jammers, such as responding to the truck based jammers deployed by the Russians and North Koreans, are not applicable to $30 jammers.[26] In 2010 the GPS landing system at Newark's Liberty International Airport was disrupted by a single truck using a GPS jammer to avoid paying road tolls.[27] The 2001 Volpe Report discussed the vast vulnerabilities of the transportation system, including air travel, to GNSS disruption.[28] In its November 2013 report to Congress, the GAO discussed the "high degree of dependence on GPS" of infrastructures, communications, energy, financial services and transportation critical infrastructures.[29]

The ground level signal received from orbiting satellites is extremely weak, on the order of -160dBW (1×10^{-16}W).[30] This signal is equivalent to viewing a 60 watt lightbulb in New York from Los Angeles.[31] By tying so many services to a single point of failure, cyber risk is substantially concentrated into a single

point of failure. These low power signals are highly susceptible to manipulation using devices that cost $30.[32] The following abuses of the satellite positioning system are routinely observed:[33]

- Jamming the signal to hide movements
- Rebroadcasting ("meaconing") a signal to misreport location
- Spoofing a signal to misreport location.

It is important to observe that these attacks are of two different types. The first, jamming, makes the information unavailable to the victim. The second, meaconing and spoofing, provides the victim with unreliable information; instead of setting off alarms, this attack methodology merely changes data, an event which may go undetected and, thus, uncorrected.[34] Defenses of data integrity, such as encryption, do not protect information availability. The attacker gets to decide if the attack will target availability, integrity or both.

The PNT whisper from space is a key terrain of cyberspace is easily overwhelmed by local sources. The disruption of the PNT signal can cascade to create havoc in the real world. In 2010 MITRE warned, [35]

> **We have an Asymmetric Vulnerability as a result of our dependence [on PNT].**

The PNT signal is not the only easily disrupted electromagnetic vulnerability of the communications system. The LTE cellular networks used for wireless communications are particularly vulnerable to jamming using equipment costing as little as $650.[36] While the inability to share one's selfies hardly seems to be matter of national security, LTE provides the infrastructure for FirstNet, the nationwide public communications network for first responders. Disrupting LTE as part of an attack will cause confusion among civil defense authorities and the public, thereby reducing the response effectiveness and increasing panic. The derecho incident demonstrated how degraded availability of cellphone towers cascaded into a failure of the 911 system. The U.S. Military is also considered LTE-based networks for battlefield communication and ship-to-naval aircraft communication.[37] The authors of *LTE/LTE-A Jamming, Spoofing, and Sniffing* observe,[38]

> **This high level of vulnerability is not surprising given that LTE was not designed to become a mission-critical communications technology. However, with the rapid adoption of mobile devices and networks, LTE is going to be highly relied-upon during the next decade.**

The submarine cable network carries over 95% of the world's international communications traffic.[39] These cables carry global business worth more than $10 trillion a day; any significant disruption would cut the flow of capital.[40] The location of these cables is readily determinable on the internet.[41] Historically, the greatest threats to the submarine cables were posed by nature, fishing gear and anchors.[42] In order to avoid inadvertent damage to the submarine cables by mariners, the locations of the cables are clearly marked on navigation charts.[43] Aids to navigation are often positioned on-shore as further assistance to mariners to avoid damaging submarine cables. In 1970, the USS *Halibut* (SSN-587) located the Soviet's undersea cable in the Sea of Okhotsk using on-shore warning signs.[44] The various aids to navigation to assist mariners serve as signposts for cyber warriors. Of course, the cables must terminate on land. The cable landing infrastructure is highly susceptible to kinetic attack.[45] The submarine cables also provide opportunities for surreptitious monitoring of cyberspace.[46] *The New York Times* reports that the Russians are surveying the submarine cable network.[47]

Under traditional military geography analysis, Bab al-Mandab, a narrow strait between Djibouti and Yemen, is a strategic chokepoint to the world's shipping.[48] More than 4% of the world's oil production flows through the strait.[49] Several Saudi ships have been sunk in this region by Yemeni forces.[50] After attacks on US Naval vessels, the US launched missile attacks on Yemini forces.[51] The US is providing covert assistance to Saudi forces to control Bab al-Mandab.[52] The risks to shipping from shore batteries are reminiscent of Washington's redoubts at West Point.

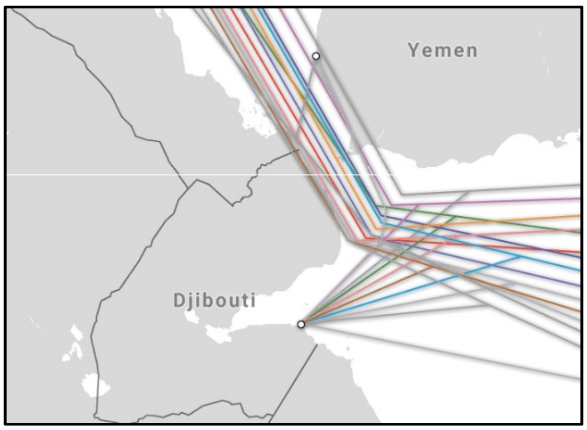


Figure 4 Bab al-Mandab Submarine Cables. Source: TeleGeography

The military geography of cyberspace at Bab al-Mandab, like the conventional military geography of Bab al-Mandad, is strongly dictated by the physical geography of the region. Figure 4 illustrates the submarine cables under Bab al-Mandab.[53] Clicking a cable displayed on the *TeleGeography* website provides the world-wide routing of that cable, its shore terminations and the URL of the cable's operator. The cable operator's website provides a wealth of information about the cable.[54]

Clearly, cutting submarine cables can disrupt data communications. For example, when two cables were cut off of the coast of Egypt in 2008, Egypt, India, Pakistan and Kuwait were left without internet.[55] The 26 December 2006 Hengchun earthquake damaged nine submarine cables in the Strait of Luzon.[56] The International Cable Protection Committee reported that the damage to these nine cables degraded the internet links in the region, impairing communications between China, Hong Kong, Singapore, Taiwan, Japan and the Philippines, severely impacting financial markets, commerce and general communications.[57] Even rerouting traffic through undamaged cables still left traffic impaired. It took eleven ships forty-nine days to restore normal operation. Cyberspace is subject to kinetic attack on the submarine telecommunications network.[58] A coordinated attack on the submarine cables could deny or degrade the system, throwing communications into chaos. The submarine cable network is another kinetic avenue of approach in cyberspace.

The physical locations where data are stored are subject to attack. Attacking data centers with the purpose of destruction is a relatively straightforward kinetic operation, akin to attacking any other facility. Kinetic damage to a data center destroys or degrades its operations. The facilities can be physically infiltrated with data transmission devices such as thumbdrives. A less dramatic attack on the physical data storage infrastructure is the theft of portable computers. Recently, the theft of a single laptop computer compromised the personnel records of over 130,000 members of the U.S. Navy.[59] According to Verizon, 2.5% of breaches are the result of the theft or loss of devices.[60] In the theft of a data storage device, data is directly accessible by the attacker without the need to navigate the logical network layer. Stuxnet demonstrates the use of a self-contained data container to physically introduce exploits into a target system.

Data that is being transferred over the internet is subject to interception. Unencrypted data, including user name and passwords, can be collected.[61] Defects in data encryption, such as the "heartbleed" defect, render information subject to disclosure. Attackers can set up wireless access points that trick users into accessing the internet using attacker resources or charging stations that steal data or corrupt device through the USB connection.[62] Attackers can use cellphones to collect data from the display components of air-gapped computers.[63]

The physical layer of cyberspace provides key terrain with clear avenues of approach. The adoption of new technologies with little analysis of vulnerabilities and dependencies increases cyber risk. In 2001 the

Volpe Report sounded an important warning when it observed that "**increasing reliance on evolving systems can lead to serious consequences if the services are disrupted and there is a lack of preparedness with mitigation equipment and operational procedures."**[64]

***Attack the Logical Network Layer*.** The logical network layer is the place where traffic is routed over the internet. When a URL is requested in cyberspace, that request is routed over the physical network layer by the logical network layer. This routing function is provided by the Domain Name Server (DNS) infrastructure. The fact that DNS consumes resources forms the basis of the Denial of Service (DoS) attack in which the attacker overwhelms the victim's ability to process requests, thereby taking down or degrading the targeted resource. Attackers can also leverage third party devices to amplify a DoS attack into a Distributed Denial of Service (DDoS) attack. In the DDoS attack an army of enslaved systems is used to increase the traffic being directed against the targeted systems. The rapid growth of the Internet of Things (IoT) provides a rich opportunity to create massive armies of zombies for DDoS attacks.[65]

Voice of Internet Protocol (VoIP) continue to grow, supporting 62% of residential users and an ever increasing share of business communications.[66] VoIP is an essential component of the E911 system.[67] VoIP can be specifically targeted to disrupt communications.[68] Evolving technologies such as IPv6 will not solve the vulnerability of networks, in general, and VoIP in particular, to DDoS attacks.[69] More generally, the vulnerability of computer systems to poor coding techniques, malware and the abuse of native functions is well-known.[70] Moreover, as data transits the logical network layer it is subject to eavesdropping, redirection and modification.[71] The logical network layer provides many avenues of approach to exploit network services.

***Attack the Cyber-Persona Layer*.** Joint Publication JP3-12(R), *Cyberspace Operations*, states:[72]

> The cyber-persona layer represents yet a higher level of abstraction of the logical network in cyberspace; it uses the rules that apply in the logical network layer to develop a digital representation of an individual or entity identity in cyberspace. The cyberpersona layer consists of the people actually on the network.

Users can be: i) human beings or ii) non-person entities (NPE), such as hardware or software, that act in cyberspace.[73] The cyber-persona layer is the focus of much cyber-chicanery because cyber-persona is where command and control is exercised in cyberspace.

A classic principle of military geography is the impact of the inhabitants on the battlespace. The pervasive nature of the inhabitants of cyberspace is somewhat reminiscent of urban warfare operations in which the urban environment clutters and confuses the battlespace.[74] Carlos Marighella, author of the *Minimanual of the Urban Guerrilla*, observed, "It is an impossible problem for the police, in the labyrinthian terrain of the urban guerrilla, to catch someone they cannot see, to repress someone they cannot catch, and to close in on someone they cannot find."[75] Where are the urban guerrillas in cyberspace? Who are the urban guerrillas in cyberspace?

Figure 5 Cyberspace Guerrillas (baby monitors). Source: Wikipedia

Cyberspace guerrillas are simultaneously everywhere and nowhere because every device connected to the internet is a potential enemy.[76] On 21 October 2016 a DDoS against Dyn, the operator of a large DNS hosting service, impacted many large online services in the United States and Sweden.[77] Among the services impacted were Twitter, *The Wall Street Journal*, Netflix, PayPal and the Swedish government.[78]

In the case of the Dyn incident, the IoT devices used a user name/password combination to authenticate the user. Regrettably, every device in the Dyn incident shipped from the factory with the same unchangeable factory default username and password. This allowed the Dyn attackers to access every similar IoT device with the same user name and password and operate these devices. Once authenticated, the attacker then installed malware which converted the factory installed authorized uses into new uses. [79] In the Dyn case, the new authorized use was serving as a zombie in a DDoS attack. The same malware can also be used to convert benign consumer devices into crime proxies, routing traffic over the internet to obscure the true origins of criminal activity.[80]

The number of devices that must be co-opted in an IoT DDoS is surprisingly small. In the 20 September 2016 DDoS against KrebsOnSecurity.com, a zombie army of 24,000 devices generated peak traffic of 555 Gbps, the largest DDoS ever observed by Akamai.[81]

The stark reality of the growth of the interest of things is that this is actually the growth of the connection of a massive number of things to the internet by system administrators who are motivated by obtaining the promised consumer value (set your thermostat from your cell phone, unlock your door with your cellphone, monitor your baby, operate your coffee maker, etc.) at the lowest possible cost in terms of time, money and expertise. IoT is a problem that is growing exponentially, projected to exceed 50 billion devices by 2020.[82]

As people who couldn't set a clock on a VCR connect gadgets to the internet, will they change the factory default username and password? If they do, will they select commonly used usernames and passwords that offer little resistance to attackers?[83]

The cyberpersona layer offers many opportunities for engagement.

***Attack the Cognitive Layer*.** The cyber-persona is merely the instrument of one or more users. For example, the cyber-persona "Customer A" could be under the control of Mr. A and Mrs. A. Or "Customer A" could be under the control of Criminal Z or Criminal Z's botnot. Customer A is an example of the general problem that when an adversary controls the cyber-persona of an authorized user, the adversary will exercise the command and control of the authorized user. The management of the relationship between Customer A and the universe of command and control agents populating the cognitive layer is critical to the maneuvering of Customer A in cyberspace. Identity and Access Management (IdAM) of people, software, and other entities is a key underpinning of security in cyberspace.[84] IdAM is the control environment within the cognitive layer that associates command and control agents with resources in cyberspace.

Identity is the claimed cyber-persona; IdAM authenticates the user and authorizes the actions of the identified user. In the Customer A example, "Identity" (Identity meaning the claimed cyber-persona) occurs when the command and control agent enters username "Customer A," thereby claiming to be cyber-persona Customer A. Authentication occurs when the command and control agent provides the required authentication information, such as a password. Authorization is what takes place on the system after entry of the combination of identity and authentication, such as Customer A may transfer money from Customer A's bank account.

Poor IdAM architectures cause many problems in cyberspace resulting from a poor correlation of the intended user/authorization to the implemented user/authorization. For example, morticians are authorized to enter deaths into the national death registry. However, the determination of who is an undertaker is made by the user. Thus, anyone can exercise the death recording privileges that were intended to be granted only to morticians.[85] The IRS continues to be plagued with an online taxpayer

account system which suffers from an inadequate IdAM architecture, allowing criminals access to online taxpayer accounts.[86]

The Dyn incident illustrates the interaction between cyber-persona and users. In the case of the Dyn incident, the tens of millions of Internet of Things (IoT) devices were sold to consumers. When consumers installed these IoT devices, the devices were attached to the internet, becoming elements of the all four layers of cyberspace:

- The physical network layer – The device itself
- The logical network layer – The network and subdivisions of the network of which the device is a member
- The cyber-persona layer – the user who is represented by rules in the logical network layer.
- The cognitive network layer -- where command and control agents exercise command and control authority over the other three layers through cyber-personas.

During the Dyn incident, the adversary used the IdAM of the IoT devices to take control of and repurpose IoT devices.

Applied Cyber Military Geography

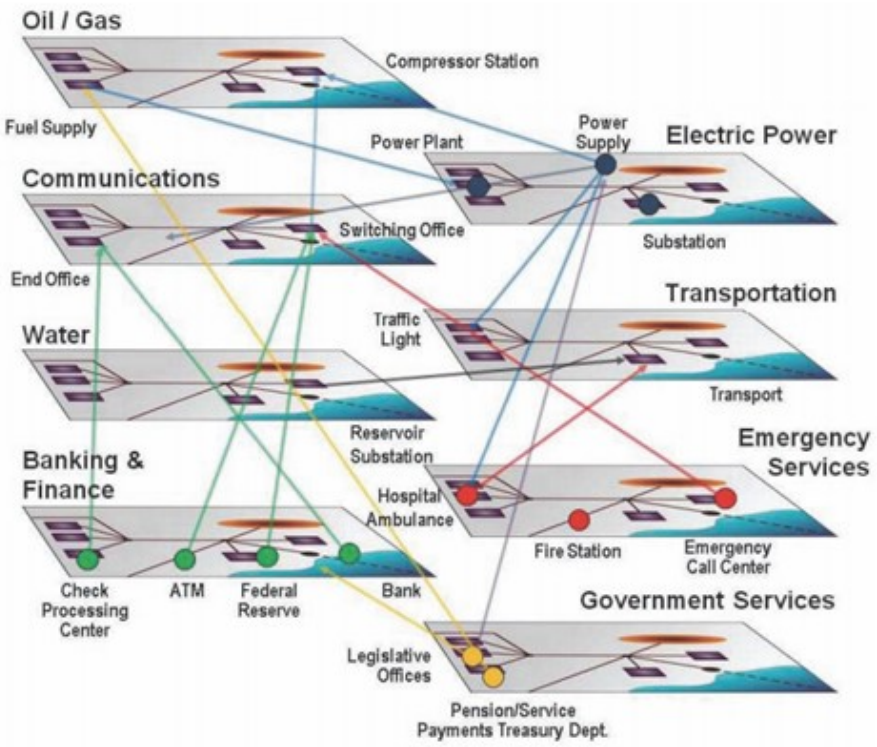
It is safe to say that no one has planned for, and few have even imagined, a scenario with the loss of hundreds or even thousands of nodes across all the critical national infrastructures, all simultaneously.

- 2008 Graham Commission Report[87]

The growing interdependence of critical infrastructures enables disruption to propagate causing cascading failures.[88] When a fiber cable was accidentally cut in January 1991, the long-distance calling capacity into and out of New York City was reduced by 60 percent, the degradation of voice and data links to air traffic control centers almost completely disabled air traffic control functions in New York, Washington, and Boston, and trading on the New York Mercantile Exchange together with several commodities exchanges was disrupted by communications failures.[89]

The Commission to Assess the Threat to the United States from Electromagnetic Pulse (EMP) Attack, chaired by Dr. William Graham, is a federal commission established to assess risks, vulnerabilities, defensive capabilities and hardening strategies respecting attacks on the United States posed by the electromagnetic pulse (EMP) that would result from the high altitude detonation of a nuclear device. Pursuant to its legislative mandate, the Commission has released two reports, the 2004 Graham

Report[90] and the 2008 Graham Report.[91] The 2008 Graham Commission provides figure 6 to illustrate the interdependence of the nation's critical infrastructure.



A Conceptual Illustration of the Interconnectedness of Elements Contained Within Each Critical Infrastructure. *Some connections are not shown (diagram provided courtesy of Sandia National Laboratory).*

Figure 6 Interconnectedness of Critical Infrastructure. Source 2008 Graham Report

Figure 6 shows how a power failure cascades across seven other critical infrastructures with devastating effects. Starting with the compromise of the electrical grid and the damage of control computers attached to the power grid, a cascading failure event can ripple through the interconnected critical infrastructure taking down broad swaths of the critical infrastructure. **A similar cascading failure starting, with compromising the power grid, can be initiated without a nuclear device using electromagnetic methods to corrupt the PNT timing signal used to synchronize the power grid.** [92]

The separation of these infrastructures into different domains tends to obscure the interdependencies that sustain the effectiveness and daily operation of each one.[93] Cyberspace, "the interdependent networks of information technology infrastructures and resident data, including the Internet, telecommunications networks, computer systems, and embedded processors and controllers,"[94] is often the foundation of the interdependencies of critical infrastructure. As figure 7 from Joint Publication

2-01.3, *Joint Intelligence Preparation of the Operational Environment,* illustrates, the information environment, of which cyberspace is a part, bridges all aspects of the operating environment.

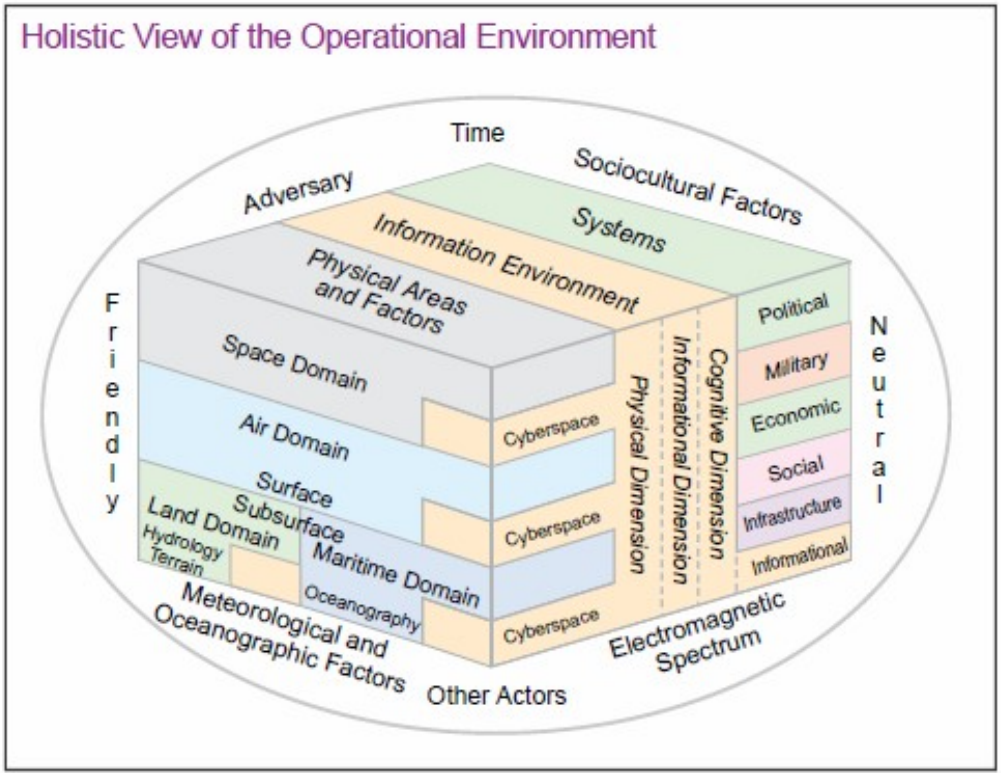


Figure 7 Holistic View of the Operational Environment. Source: JP 2-01.3

Instead of a nuclear attack or electromagnetic attack, an adversary can use command and control functions of cyberspace to leverage the interdependence of systems to intentionally propagate disruption over physical systems. For example, in December 2015, someone used a cyberattack to bring down the electric grid in Ukraine.[95] The incident commenced with an email appearing to be from the Ukrainian government to a power grid operator, however, the email actually came from the adversary. By interacting with an email, the authorized user initiated malicious processes which provided a valid user name and password to the attacker – the IdAM was compromised. **The multistep attack methodology which gains access through the cognitive layer using a spearphishing email and then guides the authorized user through a series of steps to compromise a system is the most common cyberattack methodology.**[96] With the user name and password in the possession of the authorized user and the attacker, the cyberpersona layer came under the independent control of the authorized user and the attacker. The attacker changed the password, rendering the authorized user's credentials worthless. The attacker then proceeded to use the authorized user's command and control privileges to take down the power grid, as the authorized user helplessly watched events unfold on his screen, unable to intervene for want of the new password. The attacker was able to plunge over 700,000 people into darkness, disrupting all services driven from the power grid. As part of this coordinated attack, the company's call center was overwhelmed with calls that interfered with the collection of power outage data from customers. The critical factors in the success of this attack occurred outside of the classic three layers of cyberspace, occurring in the proposed cyber cognitive layer. The propagation of this attack and the resulting impacts were contained by the lack of centralized automated control in the Ukrainian power grid, this lack of automation limited the scope of centralized administration and provided a system of distributed manual controls for grid management. This incident demonstrates an

adversary exploiting the interconnected nature of cyberspace and critical infrastructure to physical systems.

Reports now attribute the 2008 Turkish pipeline blast to the interconnectedness of systems.[97] The adversary gained access to the pipeline command and control systems through the security camera system. Having gained control of the pipeline's industrial controllers, the attackers issued commands that caused the pipeline to explode. Assuming these reports are correct, it is somewhat ironic that the pipeline was compromised through its security system.

Stuxnet malware focused on seizing the command and control of specific Siemens industrial control computers.[98] In 2010, Stuxnet caused the self-destruction of Iranian centrifuges being used to enrich nuclear materials by reprogramming the industrial controllers. Stuxnet was introduced into the Iranian systems on USB devices that were plugged into computers that were interconnected to the centrifuges. The airgapped tubes were accessed by tricking an authorized user into intruding an unauthorized device, and its software payload, into the secure system. The initial avenue of approach in this attack was the cognitive layer. Until the user introduced Stuxnet into the network, Stuxnet was harmless.

Stuxnet also reveals how connected supposedly unconnected systems are and the corresponding dangers of offensive use of malware. Air-gapped systems communicate with one another through storage media such as USB drives and other portable storage devices. When removable media is installed on a contaminated air gapped system, that removable media can be contaminated. If that contaminated media is subsequently introduced into a non-air-gapped system, the malware can spread over the entire connected environment. Any storage media installed on this contaminated environment can be contaminated. And this process of propagation can continue indefinitely. It is through this process of users unintentionally moving data to and from airgapped systems that nuclear facilities in Russia were infected with Stuxnet.[99] Astronauts introducing contaminated storage media appears to have contaminated systems on the International Space Station more than once.[100]

In November 1999, San Diego County Water Authority and San Diego Gas and Electric lost remote control of critical valves required to operate the aqueduct system. The system controlled the flow of 825 million gallons of water per day. Disaster was averted by sending technicians to remote locations to manually operate the valves. Much like the Ukrainian power grid incident, disaster was averted by the availability of manual controls, a sufficient number of personnel trained in manual operation and the availability of a communications system to coordinate the manual recovery efforts. The cause of the loss of control of was later attributed to ship's radar operating 25 miles off the coast of San Diego.[101]

NSTCS observed,[102]

> The sophistication and reach of the global communications infrastructure increase the complexity of the threat, whereas the adversary's barrier to entry is low as a result of anonymity, connectivity, and widespread availability of tools for creating disruptions.

In August of 2015, the NSA released its Adversary Obstruction Methodology.[103] The Adversary Obstruction Methodology focuses on the actions undertaken by human adversaries during engagements in cyberspace. The Adversary Obstruction Methodology introduces the terms, Access, Persistence and Control, to describe the evolution of a cyber engagement. These terms are the cyber-analogs of traditional military geography lexicon.

> Access (A) refers to how an intruder connects to your network, often enabled by poor basic security practices by employees. The intruder then aims for persistence (P) by creating a "foothold" in the network to allow a sustained presence. All of these actions are focused on

gaining control (C) to achieve the final objective, whether it is to interfere, monitor, steal or alter data, deceive, disable or destroy.[104]

The Adversary Obstruction Methodology is designed to decrease the tools, tactics and procedures that an adversary can employ against a target. Rather than the silo approach of critical infrastructure sectors which mirror lines of authority or regulation, the Adversary Obstruction Methodology applies the military geography of cyberspace to analyze the cyber engagement. The Adversary Obstruction Methodology addresses system interdependence created by cyberspace's pervasive communication, command and control network.

Applying the Adversary Obstruction Methodology to a modern car demonstrates how the Adversary Obstruction Methodology uses the military geography of cyberspace, rather than arbitrary silos, to reveal the system interdependencies surrounding a car. Figure 8 illustrates the military geography of a modern automobile. Researchers catalogued nineteen ways to access a car.[105]

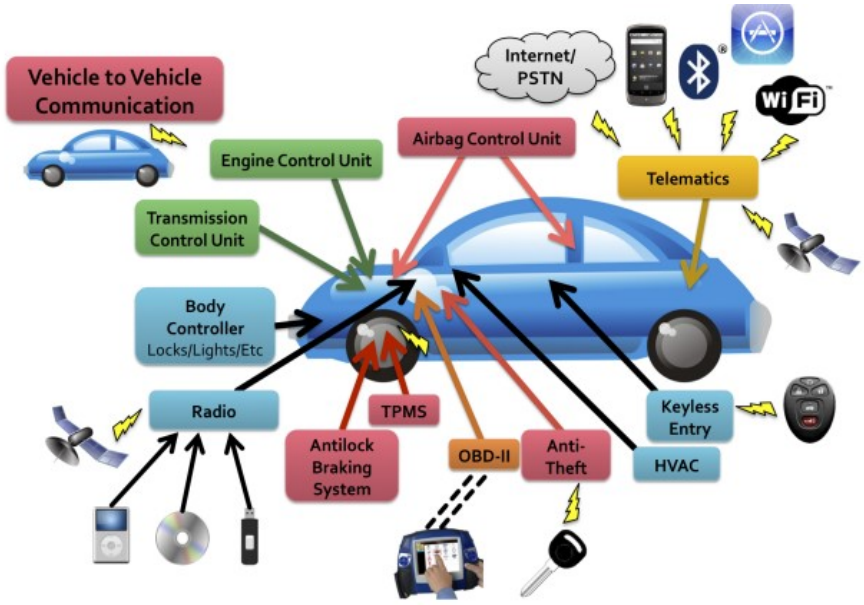


Figure 8 Access to Car. Source: Comprehensive experimental analyses of automotive attack surfaces

In addition to being subject to direct attack, the automobile itself is a node on the internet of things, which makes the car a means of access that can be used to disrupt other systems. For example, having achieved access to a car, an adversary could install a GPS jammer, using the car to establish a persistent on-demand mobile jamming platform in the satellite based PNT ecosystem. An adversary could then use this jamming platform to operate in the PNT infrastructure. Instead of starting the analysis by assigning the car to a critical infrastructure sector, the Adversary Obstruction Methodology explores how the car interacts with the four layers of cyberspace. A fleet of cars can be a deployed as mobile satellite jamming/spoofing system.[106] Real time intelligence from social networking of navigation systems can be used by adversaries for reconnaissance[107] or to misdirect friendly forces.[108] Cars could be used for targeted killings.[109] Cars could be used to impede the movement of friendly forces through the coordinated obstruction of key intersections, railroad crossings and bridges.

For George Washington, the military geography of the Hudson Valley focused on controlling the flow of men and materiel on the Hudson River. Under the Adversary Obstruction Methodology, the focus is on the flow of information over wires and the electromagnetic spectrum. The Adversary Obstruction Methodology sets forth the principles of cyber defense, which seek to limit access, persistence and

control. These principles are:[110]

- Generate a plan to respond and ensure it is fully implemented without exceptions.
- Reduce the attack surface to reduce external attack vectors into the network
- Harden devices to reduce internal and external attack vectors into the network
- Implement Credential Protections to degrade the adversaries' ability to maneuver on the network
- Align defensive resources to improve detection of and response to adversary activity
- Segregate networks and functions to contain damage when an intrusion occurs
- Develop a culture of cyber professionalism, to include leaders who set expectations

Tesla demonstrates the application of the Adversary Obstruction Methodology in its vehicles.[111] The firm determined that a car's infotainment system provides easy access to many critical systems of a car. The tubes of the infotainment system communicated with the tubes of the car's critical control systems, providing access to the critical systems of the car. Unlike other manufacturers, Tesla segregated the vehicle control systems from the infotainment system, thereby isolating a compromise of the infotainment system and containing the damage within that system.

Evaluating access requires that defenders challenge the assumptions of their defensive strategies. The defense of the US power grid is becoming increasingly dependent upon automation and coordinated system management. [112] These defensive strategies rest on the assumption that robust communication services are available to coordinate the response. What happens if the assumed communication services are compromised by a disruption of the communications system through an attack on the communications system or the infrastructures upon which the communications system relies? In fact, attacking the communications which are required to operate the power grid is a clear means of access to disrupt the power grid.[113] Lloyd's estimates that the cascading failures that could result from a cyberattack on the U.S. power grid could result in losses of over $1 trillion.[114]

Space systems are subject to cyberattacks. Flight crews have introduced malware into the International Space Station systems by installing infected storage devices carried from Earth.[115] Unmanned systems can be compromised by transmissions from ground stations, as was the case in 2013 when NASA lost contact with the International Space Station because a planned software update inadvertently cut communications.[116] The functionality of the GPS space based system has been compromised by erroneous instructions from ground controllers.[117] Large numbers of VSAT ground stations used to communicate with satellites are connected to the internet, making the satellites subject to cyberattack through the ground control infrastructure.[118] The same email methodology that compromised the Ukrainian power grid could be applied to space systems.[119]

In operations in Ukraine, the Russians have effectively compromised critical infrastructure sectors using cyberspace. Disabling the power grid, as described above, by using the cognitive layer to seize control of the power grid, is only one example of using cyberspace to impact critical infrastructure. The Russians used GPS jammers, disrupting cyberspace through the GPS system, to interfere with unmanned drone operations.[120] The Russians engaged in a coordinated multi-pronged attack on Ukraine's communications sector, with kinetic attacks on fiber optic cables and central offices, jamming the electromagnetic spectrum, VoIP packet attacks and denial of service attacks.[121] Assuming that military communications remain intact through the use of secret resources, the civilian consequences would be devastating. The Russians were able to cripple the communications of the Ukrainian legislature, substantially impairing the civilian command authority through cyberoperations.[122] The Russian's strategy assumes that Russian forces can operate in a degraded cyber-environment while its enemies cannot. Thus, the Russians are installing PNT jammers on their own cell phone towers to deny Western

forces PNT signals within Russian territory, while concurrently deploying systems that are not dependent on satellite signals.[123]

Conclusion

The shift to greater electronic controls, computers, and the Internet also results in fewer operators and different operator training. Thus the ability to operate the system in the absence of such electronics and computer-driven actions is fast disappearing.

- 2008 Graham Report[124]

The 2004 Graham Report observes:[125]

> [T]he US has developed more than most other nations as a modern society heavily dependent on electronics, telecommunications, energy, information networks, and a rich set of financial and transportation systems that leverage modern technology. This asymmetry is a source of substantial economic, industrial, and societal advantages, but it creates vulnerabilities and critical interdependencies that are potentially disastrous to the United States.

While the Graham Reports focus on disruption of systems caused by nuclear attack generated EMP, similar cascading failures can be caused by attacks on cyberspace. Rather than using a nuclear detonation to access and disrupt cyberspace, an adversary can access cyberspace using PNT jammers, LTE jammers, thumbdrives, websites and email.

Vladislav Sherstuyuk, a retired general who heads the Institute of Information Security Issues at Moscow State University and sits on Russia's National Security Council, observed,[126]

> Today we are talking about information weapons, about cyberweapons, and there is much in common between nuclear and cyberweapons, because cyber weapons can affect a huge amount of people as well as nuclear. But there is one big difference between them. Cyberweapons are very cheap, almost free of charge.

Sherstuyuk failed to observe that cyberattacks have the added benefit of plausible deniability.[127]

The NSA Adversary Obstruction Methodology provides a cyberspace specific implementation of military geography. The Access, Persistence, Control model reveals dependences which are obscured by the silo construct of discrete critical infrastructure sectors. Seeing the access provided by PNT, critical systems must be protected from the PNT tube by mitigating PNT risks.[128] Similar concerns apply to the increasing reliance on LTE for essential communication services. The proposed cognitive layer describes a means of access to the other layers of cyberspace. Credentials, the foundation of IdAM, must be well-conceived and then defended from military deception operations such as spearphishing emails.[129]

The convenience afforded by connectivity needs to be weighed against the risks introduced by reliance on fragile technology.

The views expressed herein are the views of the authors and do not reflect the views of PepsiCo, Inc. or Iconix, Inc.

Robert Zager is an inventor and entrepreneur. He has been granted eleven United States patents in the areas of computer networking and email. He holds a BA degree from the University of California, Berkeley and a JD degree from Santa Clara University. He is currently a security researcher at Iconix, Inc. in San Jose, California.

John Zager is a psychologist with a penchant for systems analysis. He holds a BA degree in Psychology and an MA degree in Industrial Organizational Psychology from Hofstra University While completing his undergraduate studies he served as an intern for U.S. Senator Kirsten Gillibrand (D, NY). He is currently a financial analyst at PepsiCo, Inc. in White Plains, New York.

[1] Gerald C. Stowe and Jac Weller, Revolutionary West Point: "The Key to the Continent." *Military Affairs*, 19: 81-92
[2] Unless otherwise noted, the discussion of Washington and West Point is drawn from Stowe, fn. 2.
[3] Collins, John M. *Military Geography: For Professionals and the Public*. Washington, DC: National Defense University Press, 1998. Print. Page XIX.
[4] Collins, fn. 5, Page 3.
[5] Palco, Col. Eugene, and Lt. Col. Frances Galgano. "The Military Geography of Fortress West Point." *West Point*. 2008. Web. 23 Jan. 2017. <http://www.westpoint.edu/gene/siteassets/sitepages/publications/the%20military%20geography%20of%20fortress%20west%20point%202001.pdf>.
[6] See Collins, fn. 3, for a comprehensive discussion of the topic of Military Geography before the emergence of the concept of "cyberspace."
[7] Doctorow, Cory. *Sen. Stevens' hilariously awful explanation of the Internet*. Boing, 2 July 2006. Web. 23 Jan. 2017. <http://boingboing.net/2006/07/02/sen-stevens-hilariou.html>.
[8] "GE 301 introduction to military geology defense of west point on the Hudson, 1775 – 1783." *Missouri University of Science and Technology*. 2004. Web. 23 Jan. 2017. <http://web.mst.edu/~rogersda/umrcourses/ge342/West%20Point%20Fortifications.pdf>.
[9] Landauer, Rolf. "Information is a physical entity." Physica A: Statistical Mechanics and its applications 263.1 (1999): 63-67.
[10] "Stuxnet." *Wikipedia*. N.p.: Wikimedia Foundation, 22 Jan. 2017. Web. 23 Jan. 2017. <https://en.wikipedia.org/wiki/Stuxnet>.
[11] JP 3-12(R), *Cyberspace Operations,* Pages I-2 – I-3.
[12] JP 3-12(R), Page I-5.
[13] The White House. *NATIONAL STRATEGY FOR TRUSTED IDENTITIES IN CYBERSPACE*. Washington, D.C., 2011. Web. 23 Jan. 2017. <http://web.archive.org/web/20170109174756/https://www.whitehouse.gov/sites/default/files/rss_viewer/NSTICstrategy_041511.pdf>.
Naudus, Stan. *The PKE Quarterly Post*. N.p.: DoD PKE, 2009. Web. 24 Jan. 2017. <http://iasecontent.disa.mil/pki-pke/DoD_PKE_Newsletter_Fall09.pdf>.
[14] For an entertaining tour of the physical components of the internet, see, Blum, Andrew. *Tubes: A Journey to the Center of the Internet*. New York: HarperCollins Publishers, 2013. Print.
[15] Graham (Chairman), Dr. William R. *Report of the Commission to Assess the Threat to the United States from Electromagnetic Pulse (EMP) Attack: Volume 1: Executive Report*. N.p.: Commission to Assess the Threat to the United States from Electromagnetic Pulse (EMP) Attack, 2004. Web. 24 Jan. 2017. <http://www.empcommission.org/docs/empc_exec_rpt.pdf>. Page 1.
[16] BBC. "Planning the US "Long War" on terror." *BBC Americas*. 10 Apr. 2006. Web. 24 Jan. 2017. <http://web.archive.org/web/20160114235419/http://news.bbc.co.uk/2/hi/americas/4897786.stm>.
[17] "Critical Infrastructure Sectors." *Department of Homeland Security*. 30 Dec. 2016. Web. 24 Jan. 2017. <https://www.dhs.gov/critical-infrastructure-sectors>. The sixteen critical infrastructures are:

- Chemical Sector
- Commercial Facilities Sector
- Communications Sector
- Critical Manufacturing Sector
- Dams Sector
- Defense Industrial Base Sector
- Emergency Services Sector

- Energy Sector
- Financial Services Sector
- Food and Agriculture Sector
- Government Facilities Sector
- Healthcare and Public Health Sector
- Information Technology Sector
- Nuclear Reactors, Materials, and Waste SectorSector-Specific Agencies
- Transportation Systems Sector
- Water and Wastewater Systems Sector

[18] "Communications Sector." *Department of Homeland Security*. 30 Dec. 2016. Web. 24 Jan. 2017. <https://www.dhs.gov/communications-sector>.
[19] Public Safety and Homeland Security Bureau. *Impact of the June 2012 Derecho on Communications Networks and Services: Report and Recommendations*. N.p.: Federal Communications Commission, Jan. 2013. Web. 24 Jan. 2017. <https://apps.fcc.gov/edocs_public/attachmatch/DOC-318331A1.pdf>.
[20] Hambling, David. "GPS chaos: How a $30 box can jam your life." *New Scientist*. Relx Group, 4 Mar. 2011. Web. 24 Jan. 2017. <https://www.newscientist.com/article/dn20202-gps-chaos-how-a-30-box-can-jam-your-life>.
[21] Caverly, R. James. "GPS critical infrastructure usage/loss impacts/backups/mitigation." *Resilient Navigation and Timing Foundation*. 2011. Web. 24 Jan. 2017. <http://rntfnd.org/wp-content/uploads/James-Caverly-DHS-GPS-PNTTimingStudy-SpaceWeather4-27-111.pdf>.
[22] Thomas (Chairman), Dr Martyn. *Global Navigation Space Systems: Reliance and Vulnerabilities*. London, England: The Royal Academy of Engineering, Mar. 2011. Web. 24 Jan. 2017. <http://www.raeng.org.uk/publications/reports/global-navigation-space-systems>.
[23] Powers, Edward. *Applications of GPS Provided Time and Frequency and Future*. Washington, D.C.: United States Naval Observatory & Naval Meteorology and Oceanography Command, 2012. Web. 24 Jan. 2017. <http://www.gps.gov/governance/advisory/meetings/2012-08/powers.pdf>.
[24] Gallagher, Sean. "North Korea pumps up the GPS jamming in week-long attack." *Ars Technica*. Conde Nast, 9 May 2012. Web. 24 Jan. 2017. <http://arstechnica.com/information-technology/2012/05/north-korea-pumps-up-the-gps-jamming-in-week-long-attack/>.
Abz, Rus. "GPS jammer attack causes the U.S. RC-7B aircraft emergency landing." *GPS4US*. 13 Sept. 2011. Web. 24 Jan. 2017. <https://www.gps4us.com/news/post/GPS-jammer-attack-causes-the-US-RC-7B-aircraft-emergency-landing-20110913.aspx>.
Evans, Stephen. "North Korea "jamming GPS signals" Near South Border." *BBC Asia*. BBC News, 1 Apr. 2016. Web. 24 Jan. 2017. <http://www.bbc.com/news/world-asia-35940542>.
[25] Mitch, Ryan H, et al. *Signal Characteristics of Civil GPS Jammers*. Portland, Oregon: ION GNSS 2011: 24th Institute of Navigation GNSS Conference, 2011. Web. 24 Jan. 2017. <https://gps.mae.cornell.edu/Paper_C3_3_ION_GNSS_2011b.pdf>.
[26] Brown, Alison, et al. *JAMMER AND INTERFERENCE LOCATION SYSTEM – DESIGN AND INITIAL TEST RESULTS*. Nashville, TN: ION GPS 1999, 1999. Web. 24 Jan. 2017. <http://www.navsys.com/Papers/9909005.pdf>.
Hambling, fn. 20.
[27] Hambling, fn. 20.
[28] John A. Volpe National Transportation Systems Center. *VULNERABILITY ASSESSMENT OF THE TRANSPORTATION INFRASTRUCTURE RELYING ON THE GLOBAL POSITIONING SYSTEM Final Report*. Cambridge, Massachusetts: U.S. Department of Transportation, 2001. Web. 24 Jan. 2017. <http://www.navcen.uscg.gov/pdf/vulnerability_assess_2001.pdf>.
[29] U.S. Government Accountability Office. *GPS DISRUPTIONS Efforts to Assess Risks to Critical Infrastructure and Coordinate Agency Actions Should Be Enhanced Report to Congressional Requesters United States Government Accountability Office*. Washington, D.C.: U.S. Government Accountability Office, Nov. 2013. Web. 24 Jan. 2017. <http://www.gao.gov/assets/660/658792.pdf>.
[30] Thomas, fn. 22 at page 5.
[31] Kim, Jason. *National PNT Advisory Board Comments on Jamming the Global Positioning System - A National Security Threat: Recent Events and Potential Cures*. N.p.: National PNT Advisory Board, 4 Nov. 2010. Web. 24 Jan. 2017. <https://danieldeubank.files.wordpress.com/2012/12/jamming-gps-4-nov-2010.pdf>.
[32] Hambling, fn. 20.

[33] Thomas, fn. 22.
[34] Starr, Michelle. "Students hijack US$80m yacht with GPS spoofing - Roadshow." *Roadshow*. CNET, 29 July 2013. Web. 25 Jan. 2017. <https://www.cnet.com/roadshow/news/students-hijack-us80m-yacht-with-gps-spoofing/>.

"Cockrell school researchers demonstrate First successful "Spoofing" of UAVs - Cockrell school of engineering." *University of Texas at Austin, Cockrell School of Engineering*. 27 June 2012. Web. 25 Jan. 2017. <http://www.engr.utexas.edu/features/humphreysspoofing>.
[35] Airst, Malcolm J. *GPS Network Timing Integrity*. N.p.: MITRE Corporation, 2010. Web. 25 Jan. 2017. <http://www.gps.gov/governance/advisory/meetings/2012-08/airst.pdf>.
[36] Talbot, David. "One simple trick could disable a city's 4G phone network." *MIT Technology Review*. MIT, 14 Nov. 2012. Web. 25 Jan. 2017. <https://www.technologyreview.com/s/507381/one-simple-trick-could-disable-a-citys-4g-phone-network/>.

Marc Louis Lichtman, et al, LTE/LTE-A jamming, spoofing, and sniffing: threat assessment and mitigation, IEEE Communications Magazine 54(4):54-61 · April 2016
[37] Lichtman, Marc, et al. "LTE/LTE-A Jamming, Spoofing, and Sniffing: Threat Assessment and Mitigation." *IEEE Communications Magazine* 54.4 (2016): 54–61. 25 Jan. 2017. <http://www.ee.columbia.edu/~roger/LTE_Jamming_Magazine_Paper_final.pdf>.
[38] Lichtman, fn. 37.
[39] "2015 ICPC Plenary Supported by Key Industry Players." Lymington, United Kingdom: International Cable Protection Committee, 26 Mar. 2015. Web. 25 Jan. 2017. <https://www.iscpc.org/documents/?id=1832>.
[40] Sanger, David E., and Eric Schmitt. "Russian Ships Near Data Cables Are Too Close for U.S. Comfort." *Europe*. The New York Times, 26 Oct. 2015. Web. 25 Jan. 2017. <https://web.archive.org/web/20160313231419/http:/www.nytimes.com/2015/10/26/world/europe/russian-presence-near-undersea-cables-concerns-us.html?hp&action=click&pgtype=Homepage&module=first-column-region&region=top-news&WT.nav=top-news&_r=0>.
[41] "Submarine cable map." *TeleGeography*. PriMetrica, Inc., 21 Jan. 2017. Web. 25 Jan. 2017. <http://www.submarinecablemap.com/#/>. TeleGeography is one of the open interactive mapping services that provides interactive maps of the submarine telecommunications network.
[42] Carter L., Burnett D., Drew S., Marle G., Hagadorn L., Bartlett-McNeil D., and Irvine N. (2009). *Submarine Cables and the Oceans – Connecting the World*. UNEP-WCMC Biodiversity Series No. 31. ICPC/UNEP/UNEP-WCMC.
[43] "Nautical charts & pubs." *NOAA Office of Coast Survey*. 6 Dec. 1995. Web. 25 Jan. 2017. <http://www.charts.noaa.gov/>.
[44] Sontag, Sherry, Christopher Drew, and Annette Lawrence Drew. *Blind Man's Bluff: The Untold Story of American Submarine Espionage*. New York: PublicAffairs, U.S., 1998. Print. Page 170.
[45] Protective Security Division. *CHARACTERISTICS AND COMMON VULNERABILITIES INFRASTRUCTURE CATEGORY: CABLE LANDING STATIONS CABLE LANDING STATION CHARACTERISTICS*. N.p.: Department of Homeland Security, 15 Jan. 2004. Web. 25 Jan. 2017. <http://info.publicintelligence.net/DHS-UCL-CV.pdf>.
[46] Sontag, fn. 44.

Axe, David. "This is the U.S. Navy's most secretive submarine." *The Week*. 20 Aug. 2015. Web. 25 Jan. 2017. <http://theweek.com/articles/572513/isthe-navys-most-secretive-submarine>.
[47] Sanger, fn. 40.

[48] Al-Yadoomi, Colonel Staff Hussain. *THE STRATEGIC IMPORTANCE OF THE BAB AL-MANDAB STRAIT*. Carlisle Barracks, Pennsylvania: United States Army War College, Apr. 1991. Web. 25 Jan. 2017. <http://www.dtic.mil/dtic/tr/fulltext/u2/a236804.pdf>.

Mello, Alexandre, Cmdr. Jeremy Vaughn, USN, and Michael Knights. "Houthi Antishipping attacks in the Bab al-mandab strait." *The Washington Institute*. 6 Oct. 2016. Web. 25 Jan. 2017. <http://www.washingtoninstitute.org/policy-analysis/view/houthi-antishipping-attacks-in-the-bab-al-mandab-strait>.

Presse, Agence France. “Sissi says securing Yemen’s key strait an Egypt priority.” *Arab News*. Saudi Research and Publishing Company, 5 Apr. 2015. Web. 25 Jan. 2017. <http://www.arabnews.com/middle-east/news/727751>.
[49] Metelitsa, Alexander, and Megan Mercer. “World oil transit chokepoints critical to global energy security - today in energy - U.S. Energy information administration (EIA).” *U.S. Department of Energy*. 1 Dec. 2014. Web. 25 Jan. 2017. <http://www.eia.gov/todayinenergy/detail.php?id=18991>.
[50] Al-Alam News Network. “Yemeni troops drown Second Saudi warship.” *11 October 2015*. 11 Oct. 2015. Web. 25 Jan. 2017. <http://en.alalam.ir/news/1747675>.

[51] "U.S. Navy Operations in a Maritime Chokepoint." *CFR.org*. Council on Foreign Relations, 20 Oct. 2016. Web. 6 Nov. 2016. <http://www.cfr.org/middle-east-and-north-africa/us-navy-operations-maritime-chokepoint/p38421>.
[52] Nas, Francheska Lyn. ““Yemen files” exposed by WikiLeaks, reveals hidden US role.” *GeoPolMonitor*. GEOPOLMonitor, 28 Nov. 2016. Web. 25 Jan. 2017. <http://www.geopolmonitor.com/yemen-files-exposed-wikileaks-reveals-us-hidden-role/>.
[53] TeleGeography, fn. 41.

[54] SEA-ME-WE-5. “SEA-ME-WE-5 submarine cable system & consortium.” *SEA-ME-WE 5*. SEA-ME-WE 5, 2015. Web. 25 Jan. 2017. <http://www.seamewe5.com/>.
[55] Singel, Ryan. “Fiber Optic Cable Cuts Isolate Millions From Internet, Future Cuts Likely.” *Security*. WIRED, 31 Jan. 2008. Web. 25 Jan. 2017. <https://www.wired.com/2008/01/fiber-optic-cab/>.
[56] Marle, Graham. *Subsea Landslide Is Likely Cause of SE Asian Communications Failure*. N.p.: International Cable Protection Committee, 21 Mar. 2007. Web. 25 Jan. 2017. <https://www.iscpc.org/documents/?id=9>.
[57] Marle, fn. 56.
[58] Chang, Alexandra. “John Arnold made a fortune at Enron. Now he’s declared war on bad science.” *Gadget Lab*. WIRED, 2 Apr. 2013. Web. 25 Jan. 2017. <https://www.wired.com/2013/04/how-vulnerable-are-undersea-internet-cables/>.
[59] Mathews, Lee. “One Laptop Has Leaked Private Data on 130, 000 Navy Sailors.” *Forbes*. Forbes, 24 Nov. 2016. Web. 25 Jan. 2017. <http://www.forbes.com/sites/leemathews/2016/11/24/one-laptop-has-leaked-private-data-on-130000-navy-sailors/#22416eb24199>.
[60] Enterprise, Verizon. *2016 Data Breach Investigations Report*. N.p.: Verizon Enterprise Solutions, 27 Apr. 2016. Web. 25 Jan. 2017. <http://www.verizonenterprise.com/resources/reports/rp_DBIR_2016_Report_en_xg.pdf>. Page 23.
[61] Krebs, Brian. “Security fix - wireless awareness: Don’t be A sheep.” *The Washington Post*. 2008. Web. 25 Jan. 2017. <http://voices.washingtonpost.com/securityfix/2008/08/wireless_awareness_dont_be_a_s.html>.
[62] Krebs, fn. 61.

McGinley, Elizabeth, et al. “Juice jacking: Did that “free” charging station just steal your data?” *Inside Counsel*. 13 June 2014. Web. 25 Jan. 2017. <http://www.insidecounsel.com/2014/06/13/juice-jacking-did-that-free-charging-station-just?slreturn=1485381533>.
[63] Zetter, Kim. *These researchers just hacked an air-gapped computer using a simple Cellphone*. Slate Magazine, 27 July 2015. Web. 23 Jan. 2017. <http://www.slate.com/blogs/future_tense/2015/07/27/air_gapped_computers_these_israeli_researchers_just_hacked_one_with_a_cell.html>.
[64] Volpe Report, fn. 28. Page ES 1.
[65] FP_Analyst. “Flashpoint - attack of things!” *BRI*. Flashpoint, 17 Sept. 2016. Web. 25 Jan. 2017. <https://www.flashpoint-intel.com/attack-of-things/>.
[66] Myers, Diane. “RESEARCH NOTE - voice over IP services market up 5 percent in 2015 - IHS technology.” *IHS Market*. 8 Apr. 2016. Web. 25 Jan. 2017. <https://technology.ihs.com/577665/research-note-voice-over-ip-services-market-up-5-percent-in-2015>.

[67] Public Safety and Homeland Security Bureau, fn. 19.
[68] Zhang, Ge, and Simone Fischer-Hubner. “Counteract DNS Attacks on SIP Proxies Using Bloom Filters.” *2013 International Conference on Availability, Reliability and Security* (2013): 678–684. 25 Jan. 2017. <https://pdfs.semanticscholar.org/b0bd/f800911823f98f8b47162ec6d98ffb9ad5b5.pdf>.

[69] Kamra, A., et al. "The Effect of DNS Delays on Worm Propagation in an IPv6 Internet." *Proceedings IEEE 24th Annual Joint Conference of the IEEE Computer and Communications Societies.* (2005): n.pag. 25 Jan. 2017. <https://www.cs.columbia.edu/~angelos/Papers/2005/dns-worm.pdf>.
[70] Green, Andy. "Top Five most dangerous software errors." *IT Pros*. Varonis Blog, 11 Aug. 2014. Web. 25 Jan. 2017. <https://blog.varonis.com/top-five-dangerous-software-errors/>.

"Malware." *Wikipedia*. N.p.: Wikimedia Foundation, 17 Jan. 2017. Web. 25 Jan. 2017. <https://en.wikipedia.org/wiki/Malware>.

Counter Threat Unit (CTU) Research Team. "Living off the land." *SecureWorks*. 28 May 2015. Web. 25 Jan. 2017. <https://www.secureworks.com/blog/living-off-the-land>.
[71] Microsoft. "Common types of network attacks." *Microsoft TechNet*. 2017. Web. 25 Jan. 2017. <https://technet.microsoft.com/en-us/library/cc959354.aspx>.
[72] JP 3-12(R), p. I-3.
[73] The White House, fn. 13.

Naudus, fn. 13.
[74] Collins, fn. 3. Pages 119-204.
[75] Marighella, Carlo. "Minimanual of the urban guerrilla." *U.S. Marine Corps*. 1969. Web. 17 Jan. 2017. <http://www.mccdc.marines.mil/Portals/172/Docs/SWCIWID/COIN/Insurgent Principles and Practices/Mini-Manual of the Urban Guerrilla - Carlos Marighella (1969).pdf>.
[76] "2016 Dyn cyberattack." *Wikipedia*. N.p.: Wikimedia Foundation, 19 Jan. 2017. Web. 25 Jan. 2017. <https://en.wikipedia.org/wiki/2016_Dyn_cyberattack>.
[77] 2016 Dyn cyberattack, fn. 76.
[78] 2016 Dyn cyberattack, fn. 76.
[79] Krebs, Brian. "Source code for IoT Botnet "Mirai" released." *KrebsOnSecurity*. 1 Oct. 2016. Web. 25 Jan. 2017. <https://krebsonsecurity.com/2016/10/source-code-for-iot-botnet-mirai-released/>.
[80] Krebs, Brian. "IoT devices as proxies for Cybercrime." *KrebsOnSecurity*. 13 Oct. 2016. Web. 25 Jan. 2017. <https://krebsonsecurity.com/2016/10/iot-devices-as-proxies-for-cybercrime/>.
[81] Krebs, Brian. "Akamai on the record KrebsOnSecurity attack." *KrebsOnSecurity*. 22 Nov. 2017. Web. 26 Jan. 2017. <https://krebsonsecurity.com/2016/11/akamai-on-the-record-krebsonsecurity-attack/#more-36963>.
[82] Wellers, Daniel. *Is this the future of the Internet of things?* World Economic Forum, 2017. Web. 26 Jan. 2017. <https://www.weforum.org/agenda/2015/11/is-this-future-of-the-internet-of-things/>.
[83] Burnett, Mark. *Is 123456 really the most common Password?* xato: security, 22 Jan. 2015. Web. 26 Jan. 2017. <https://xato.net/is-123456-really-the-most-common-password-51cd4259927d#.2fodvgv97>.

Ferguson, Rik. "Researcher uncovers IEEE data breach, reveals poor security practices -." *Trend Micro SimplySecurity*. 28 Sept. 2012. Web. 26 Jan. 2017. <https://blog.trendmicro.com/researcher-uncovers-ieee-data-breach-reveals-poor-security-practices/>.

SH-Soft Solutions. "SECURITY: Worst usernames to use as administrator on an internet facing system." *SH-Soft Solutions*. 2016. Web. 26 Jan. 2017. <https://www.sh-soft.com/en/security/security-worst-usernames-to-use-as-administrator-on-an-internet-facing-system.html>.

Gonsalves, Antone. "Yahoo security breach shocks experts." *CSO from IDG*. IDG Communications, Inc., 12 July 2012. Web. 26 Jan. 2017. <http://www.csoonline.com/article/2131970/identity-theft-prevention/yahoo-security-breach-shocks-experts.html>.

Schwartz, Mathew J. "WordPress hackers exploit Username "Admin."" *Dark Reading*. UBM, 15 Apr. 2013. Web. 26 Jan. 2017. <http://www.darkreading.com/attacks-and-breaches/wordpress-hackers-exploit-username-admin/d/d-id/1109538>.
[84] See, Mueller (Chairman), Edward. *NSTAC Response to the Sixty-Day Cyber Study Group*. Washington, D.C.: The White House, 12 Mar. 2009. Web. 26 Jan. 2017. <http://web.archive.org/web/20170118131238/https://www.whitehouse.gov/files/documents/cyber/NSTAC%20R

esponse%20to%20the%20Sixty-Day%20Cyber%20Study%20Group%203-12-09.pdf> for a discussion of the impact of IdAM on national security and emergency preparedness respecting communications.
[85] Storm, Darlene. "Def con: How to virtually kill someone or cash in on fake babies." *Computerworld*. IDG Communications, Inc., 9 Aug. 2015. Web. 26 Jan. 2017. <http://www.computerworld.com/article/2966130/cybercrime-hacking/def-con-how-to-virtually-kill-someone-or-cash-in-on-fake-babies.html>.
[86] Krebs, Brian. "IRS: 390K more victims of IRS.Gov weakness." *KrebsOnSecurity*. 26 Feb. 2016. Web. 26 Jan. 2017. <https://krebsonsecurity.com/2016/02/irs-390k-more-victims-of-irs-gov-weakness/>.
[87] Graham (Chairman), Dr. William R. *Report of the Commission to Assess the Threat to the United States from Electromagnetic Pulse (EMP) Attack Critical National Infrastructures*. N.p.: Commission to Assess the Threat to the United States from Electromagnetic Pulse (EMP) Attack, Apr. 2008. Web. 26 Jan. 2017. <http://www.empcommission.org/docs/A2473-EMP_Commission-7MB.pdf>.
[88] Graham, fn. 87.

[89] Schneider, Fred B., ed. *Trust in Cyberspace*. September 29, 1998 Prepublication Copy ed. Washington, D.C.: National Academy Press, 1998. Web. 26 Jan. 2017. <https://www.memresearch.org/grabbe/tic.htm>.
[90] Graham, fn. 15.
[91] Graham, fn. 87.
[92] Akkaya, Ilge, Edward A. Lee, and Patricia Derler. "Model-Based Evaluation of GPS Spoofing Attacks on Power Grid Sensors." *2013 Workshop on Modeling and Simulation of Cyber-Physical Energy Systems (MSCPES)* (May 2013): n.pag. 26 Jan. 2017. <https://www.researchgate.net/publication/261455896_Model-based_evaluation_of_GPS_spoofing_attacks_on_power_grid_sensors>.
[93] Graham, fn. 87. Page 10.
[94] JP 3-12(R), Page v.
See Graham, fn. 87 for a discussion of the proliferation of industrial control systems.
[95] Lipovsky, Robert, and Anton Cherepanov. "BlackEnergy trojan strikes again: Attacks Ukrainian electric power industry." *WeLiveSecurity*. ESET, 4 Jan. 2016. Web. 26 Jan. 2017. <http://www.welivesecurity.com/2016/01/04/blackenergy-trojan-strikes-again-attacks-ukrainian-electric-power-industry/>.

Zetter, Kim. "Inside the Cunning, Unprecedented Hack of Ukraine's Power Grid." *WIRED*. Conde Nast, 3 Mar. 2016. Web. 26 Jan. 2017. <https://www.wired.com/2016/03/inside-cunning-unprecedented-hack-ukraines-power-grid/>.

Pagliery, Jose. "Scary Questions in Ukraine Energy Grid Hack." *CNN*. CNN, 18 Jan. 2016. Web. 26 Jan. 2017. <http://money.cnn.com/2016/01/18/technology/ukraine-hack-russia/index.html>.
[96] Hackett, Robert. *Data Sheet—Saturday, November 19, 2016*. Fortune, 2017. Web. 26 Jan. 2017. <http://fortune.com/2016/11/19/data-sheet-saturday-november-19-2016/>.
[97] Robertson, Jordan, and Michael Riley. "Mysterious '08 Turkey Pipeline Blast Opened New Cyberwar." *Bloomberg Technology*. Bloomberg, 10 Dec. 2014. Web. 26 Jan. 2017. <https://www.bloomberg.com/news/articles/2014-12-10/mysterious-08-turkey-pipeline-blast-opened-new-cyberwar>.
[98] Wikipedia, fn. 10.
[99] Marchant, Brian. "Stuxnet, America's nuclear plant-attacking virus, has apparently infected the international space station (update: Apparently not)." *Motherboard*. Vice Media LLC, 11 Nov. 2013. Web. 26 Jan. 2017. <http://motherboard.vice.com/blog/stuxnet-americas-nuclear-plant-attacking-virus-has-infected-the-international-space-station>.
[100] Danchev, Dancho. "Malware detected at the international space station." *ZDNet*. ZDNet, 26 Aug. 2008. Web. 26 Jan. 2017. <http://www.zdnet.com/article/malware-detected-at-the-international-space-station/>.
[101] Graham, fn. 87. Page 2.
[102] Mueller, fn. 84. Page 8.
[103] "NSA Methodology for Adversary Obstruction." *Information Assurance Directorate*. NSA/IAD, 15 Sept. 2015. Web. 26 Jan. 2017. <https://www.iad.gov/iad/customcf/openAttachment.cfm?FilePath=/iad/library/reports/assets/public/upload/NSA-Methodology-for-Adversary-Obstruction.pdf&WpKes=aF6woL7fQp3dJizXCkcbwTeLkU9HubDMyr393t>.

[104] NSA, fn. 103.
[105] Checkoway, Stephen, et al. "Comprehensive experimental analyses of automotive attack surfaces." *SEC'11 Proceedings of the 20th USENIX conference on Security*. Berkeley, California. N.p.: USENIX Association Berkeley, CA, 2011. Web. <http://www.autosec.org/pubs/cars-usenixsec2011.pdf>.
[106] Wood, Andrew. "Newark airport GBAS vulnerable to truckers' GPS Jammers." *Business Aviation*. Aviation International News, 25 Jan. 2011. Web. 26 Jan. 2017. <http://www.ainonline.com/aviation-news/business-aviation/2011-01-25/newark-airport-gbas-vulnerable-truckers-gps-jammers>.
[107] The Los Angeles police have objected to Waze because its social networking features report police locations which can be used by criminals. See, Rocha, Veronica, and Richard Winton. "L.A. Police chief goes public with concerns over Google Waze app." *Los Angeles Times*. Los Angeles Times, 28 Jan. 2015. Web. 26 Jan. 2017. <http://www.latimes.com/local/crime/la-me-0128-waze-cops-20150128-story.html>.

[108] Defense officials warn about the risks of relying on technology for real time intelligence. See, Opall-Rome, Barbara. "Israeli-soldiers-dangerous-wrong-turn-using-waze-highlights-possible-pitfalls-tech-reliance." *Defense News*. Sightline Media Group Site, 2 Mar. 2016. Web. 26 Jan. 2017. <http://www.defensenews.com/story/defense/international/mideast-africa/2016/03/02/israeli-soldiers-dangerous-wrong-turn-using-waze-highlights-possible-pitfalls-tech-reliance/81232158/>.
[109] Hogan, Mike. "Was Hastings' Car Hacked?" *Huffington Post*. The Huffington Post, 24 June 2013. Web. 26 Jan. 2017. <http://www.huffingtonpost.com/2013/06/24/michael-hastings-car-hacked_n_3492339.html?utm_hp_ref=politics>.

[110] NSA, fn. 103.
[111] "Security and the Internet of Things: When your refrigerator steals your identity." *The Next Wave* 2016: 17–21. Special Edition Vol. 21 | No. 2 | 2016. 26 Jan. 2017. <https://www.nsa.gov/resources/everyone/digital-media-center/publications/the-next-wave/assets/files/TNW-21-2.pdf>.
[112] Korkali, Mert, et al. "Title: Reducing Cascading Failure Risk by Increasing Infrastructure Network Interdependency." (24 Oct. 2014): n.pag. 26 Jan. 2017. <https://arxiv.org/abs/1410.6836>.
[113] Akkaya, fn. 92.
[114] Ruffle (Project Lead), Simon. *Business Blackout: The Insurance Implications of a Cyber Attack on the US Power Grid - July 2015*. Cambridge, United Kingdom: Lloyd's and the University of Cambridge Centre for Risk Studies, 2015. Web. 27 Jan. 2017. <http://www.lloyds.com/~/media/files/news%20and%20insight/risk%20insight/2015/business%20blackout/business%20blackout20150708.pdf>.
[115] Marchant, fn. 99.
[116] "Temporary Comm loss interrupts crew's day." *International Space Station*. NASA, 19 Feb. 2013. Web. 26 Jan. 2017. <https://www.nasa.gov/mission_pages/station/expeditions/expedition34/e34_021913.html>.
[117] Baraniuk, Chris. "GPS Error Caused "12 hours of problems" for Companies." *BBC Technology*. BBC News, 4 Feb. 2016. Web. 26 Jan. 2017. <http://www.bbc.com/news/technology-35491962>.
[118] Paganini, Pierluigi. "VSAT terminals are opened for targeted cyber attacks." *Hacking*. Security Affairs, 9 Jan. 2014. Web. 26 Jan. 2017. <http://securityaffairs.co/wordpress/21049/hacking/vsat-terminals-opened-targeted-cyber-attacks.html>.
[119] Bansal, Sudhir K. "Small Satellite Terminals (VSAT) Are Vulnerable to Cyber Attack." The Hacker News, 9 Jan. 2014. Web. 26 Jan. 2017. <http://thehackernews.com/2014/01/small-satellite-terminals-vsat-are.html>.
[120] Lynch, Colum, et al. "Russia's winning the electronic war." *Report*. Foreign Policy, 23 Sept. 2016. Web. 26 Jan. 2017. <http://foreignpolicy.com/2015/10/21/russia-winning-the-electronic-war/>.
[121] Paganini, Pierluigi. "Crimea – the Russian Cyber strategy to hit Ukraine." *General Security*. InfoSec Resources, 11 Mar. 2014. Web. 26 Jan. 2017. <http://resources.infosecinstitute.com/crimea-russian-cyber-strategy-hit-ukraine/>.
[122] Paganini, fn. 121.
[123] N, John. "Russians fit cell towers with pole-21 missile defense system." *Security*. Edgy Labs, 15 Nov. 2016. Web. 24 Jan. 2017. <https://edgylabs.com/2016/11/15/pole-21-missile-defense-system/>.

The Russians, and others, have installed systems that reduce their own reliance on satellite signals. See, Goward, Dana. "Opinion | the Looming National Security Threat Everyone Keeps Ignoring." *Washington Post*. Washington Post, 12 Jan. 2017. Web. 27 Jan. 2017. <https://www.washingtonpost.com/opinions/the-looming-national-

security-threat-everyone-keeps-ignoring/2017/01/12/1c69df44-c79c-11e6-85b5-76616a33048d_story.html?utm_term=.a5f5a8d7652c>.

[124] Graham, fn. 87. Page 124.
[125] Graham, fn. 15. Page 2.
[126] Talbot, David. "Russia's Cyber security plans." *MIT Technology Review*. MIT Technology Review, 22 Oct. 2012. Web. 26 Jan. 2017. <https://www.technologyreview.com/s/418495/russias-cyber-security-plans/>.
[127] ThreatConnect Research Team. "Guccifer 2.0: the Man, the Myth, the Legend?" *ThreatConnect*. 20 July 2016. Web. 26 Jan. 2017. <https://www.threatconnect.com/reassesing-guccifer-2-0-recent-claims/?_ga=1.85934809.1940797871.1485471809>.
[128] Donilon (Chair), Thomas E. *COMMISSION ON ENHANCING NATIONAL CYBERSECURITY REPORT ON SECURING AND GROWING THE DIGITAL ECONOMY*. Washington, D.C.: The White House, 1 Dec. 2016. Web. 27 Jan. 2017. <https://www.nist.gov/sites/default/files/documents/2016/12/02/cybersecurity-commission-report-final-post.pdf>.

Fetter, Steve, et al. *IMPLEMENTATION ROADMAP FOR THE NATIONAL CRITICAL INFRASTRUCTURE SECURITY AND RESILIENCE RESEARCH AND DEVELOPMENT PLAN*. Washington, D.C.: The White House, 15 Dec. 2016. Web. 27 Jan. 2017. <https://obamawhitehouse.archives.gov/sites/default/files/microsites/ostp/NSTC/cisr_rd_implementation_roadmap_final.pdf>.

Goward, fn. 123.

U.S. Government Accountability Office, fn. 29.
[129] Zager, John, and Robert Zager. "Improving Cybersecurity through human systems integration." *Small Wars Journal*. 22 Aug. 2016. Web. 27 Jan. 2017. <http://smallwarsjournal.com/jrnl/art/improving-cybersecurity-through-human-systems-integration>.