BERKELEY MODEL UNITED NATIONS

LXVI
SIXTY-SIXTH SESSION

US CYBERCOM

WELCOME LETTER

Hello! My name is Jake Tibbetts, I am a 2nd year double majoring in Computer Science and Global Studies. I did Model UN in Southern California for 4 years in high school and this will be my 6th year doing Model United Nations. In addition to BMUN, I am also the Director of Programming for National High School Model United Nations Conference and I'm the Director of Communications for the Office of the Chief Technology Officer of the Associated Students of the University of California. In addition to this, I am an undergraduate researcher at the Goldman School of Public Policy. Also, I love watching movies, reading about history and learning Arabic, learning how to use new programming languages and technologies, and watching stand-up comedy (I also performed stand-up for two years in high school). Please read below to learn a little bit about your vice chairs:

Nikhil Pimpalkhare is a current freshman at Cal studying Electrical Engineering and Computer Science. In BMUN, he is a member of the technology staff and also is a vice chair of CYBER! Outside of Model UN, he enjoys attending local hackathons, playing chess, and tossing frisbees. He looks forward to seeing you all at conference!

Trent Gomberg is a third year molecular biology major and computer science minor. Outside of BMUN, he volunteers in Harris lab as an undergraduate researcher,

and in his free time he enjoys climbing rocks, eating a large amounts of food, long walks on the beach, and Cyber Security Crises Committees. Needless to say, he is very excited for this committee, and you should be too!

Suchitra Narayanan (Suchi for short) and is a second year studying Chemical Engineering and Astrophysics. When she's not doing BMUN, you can find her in the Radio Astronomy Lab in Campbell Hall researching the Orion Nebula or at the Richmond Field Station building wings for the Aerodynamics team of Berkeley Formula Racing. Other stuff about her: she loves dogs, sleeping, pace, swimming, water polo, and piano. Anyway, she thinks conference is amazing and is so excited to get to know all of you!

Good luck with your research! Please let us know if you have any questions.

Jake Tibbetts

Head Chair, US CYBERCOM

Berkeley Model United Nations, Sixty-Sixth Session

US CYBERCOM

HISTORY OF CYBERSECURITY

The history of cybersecurity begins in the early 1900s with its precursor, Signals Intelligence (SIGINT). Militaries and governments began to use new mediums of communication such as the telegraph and wireless radio signals to conduct the logistics of conflict. Consequently, these militaries also began to use these mediums to intercept each other's communications to bolster their other intelligence efforts. The first instance of this can be seen as early as 1904 during the Russo-Japanese War when the HMS Diana, a British naval vessel stationed in the Suez Canal, intercepted Russian naval orders and passed them onto the Japanese (Clarke, Knake 2010).

By the dawn of WW1, signals intelligence became a common, well-established practice in the world of clandestine operations because of the proliferation of technological advancements in communications. A famous example of the use of signals intelligence is the interception of the Zimmerman Telegram, a diplomatic communique from Germany to Mexico proposing an alliance against the United States. Ultimately, this became a major factor in the US deciding to fight in WW1, turning the tide of the war in favor of France and Great Britain. In WW2, the crack of the German

Enigma Code by Alan Turing and a similar crack of Japanese Purple codes by American cryptographers and linguists helped play critical roles in the defeat of the Axis Powers. The employment of SIGINT operations during WWI and WW2 demonstrated that SIGINT operations could have potential strategic and political consequences and these operations were not just limited to tactical and operational realms (see excerpt). In short, even in WW2, SIGINT was an important part of the military and intelligence institutions of any state. Although signals intelligence is less important today, SIGINT's importance to military and intelligence efforts is continued by its successor, digital espionage. This is the reason why cybersecurity is considered to be such a pressing national security issue for a number of countries today, particularly the United States.

Excerpt from "Three Levels of War"

"Modern military theory divides war into strategic, operational and tactical levels. The strategic level focuses on defining and supporting national policy and relates directly to the outcome of a war or other conflict as a whole. The operational level is concerned with employing military forces in a theatre of war or theater of operations to obtain an advantage over the enemy and thereby attain strategic goals through the design, organization, and conduct of campaigns and major operations. The tactical level translates potential combat power into success in battles and engagements through decisions and actions that create advantages when in contact with or in proximity to the enemy." (Maxwell 1997)

During the Cold War, adversaries competed in a series of diplomatic maneuvers, proxy wars, and clandestine operations rather than a full-scale thermonuclear war. Gaining strategic advantages through the use of espionage became a common tactic of both the United States and the Soviet Union. General trends in technology made communication more efficient and reliant on vulnerable mediums that were readily exploited by newly formed intelligence organizations such as the CIA, the NSA, and the KGB (Kaplan 2016). This led to an explosion of new, lucrative opportunities in the realm of SIGINT. Despite this, human intelligence (HUMINT) was still the primary method of intelligence gathering and SIGINT remained relatively limited in scope and very secretive for the majority of the Cold War.

By the 80s, communications technology had advanced so much to the point that a number of countries began to rely heavily on the Internet and networked systems to maintain important aspects of the state. Because these technologies, primarily the Internet, were designed with efficiency rather than security in mind (Timburg, 2015) by its framers, the potential for digital intelligence gathering operations began to supersede more traditional forms of intelligence gathering. During this period these was a massive conversion of important systems, such as financial mechanisms to military command and control infrastructure, to digital technologies; with greater reliance on digital technology came greater vulnerabilities and broad-scale exploitation of those vulnerabilities. For example, in 1986, Cliff Stoll, an astronomer at the Lawrence

Berkeley National Laboratory, uncovered the first documented advanced persistent threat (APT) (Lockheed Martin 2013) which turned out to be an espionage effort by the Soviet Union to gain information on the US's Strategic Defense Initiative.

In the 90s, there was yet another new development in how states leveraged new technology: using cyber operations on the battlefield in conjunction with more conventional forms of warfare. Both in Operation Desert Storm (Kaplan) and the US Bombing of Serbia in 1999 (Kaplan), there were limited uses of SIGINT operations in conventional conflict from cutting and tapping communication lines to exploiting vulnerabilities in air defense radar systems to obfuscate the direction of incoming jets. It is during this period of time that military operations in cyberspace, aptly dubbed "cyberwarfare" or "fifth domain" (Murphy 2010) operations, began to have practical utility, albeit limited. By the end of the 90s, nearly 20 countries had some kind of cyber operations unit in their military or intelligence institutions (Clarke, Knake).

One of the most important recent developments in cybersecurity is the possibility of attacking targets existing in the physical world through digital mediums. This idea remained theoretical until 2008 when the US Department of Homeland Security commissioned the Idaho National Laboratory (Kaplan) to conduct the Aurora Generator Test; a test in which a team destroyed an electrical generator using a vulnerability in the software that controlled it.

Additionally, in 2010, Operation Olympic Games, dubbed Stuxnet by its discoverers, proved the utility of cyber operations to sabotage physical infrastructure. Approximately 1000 centrifuges at the Natanz Nuclear Reactor in Iran were destroyed by a highly sophisticated computer virus (Zetter 2014). The United States and Israel are suspected of developing and initially deploying this virus to the reactor for the purpose of setting back Iran's nuclear program. Ultimately, Stuxnet was a large-scale attack on important physical systems reliant on digital infrastructure. It showed that the "Cyber Pearl Harbor" (Ryan 2011) that alarmists theorize is not a farfetched doomsday-sayer's theory but rather it is a potential future.

In summary, we can see a number of trends in the history of cyberspace as a domain of conflict: technology driving capability and widening the scope of opportunities for governments to leverage these capabilities against each other, the use of cyberspace for not just sabotage, espionage, and subversion (Rid 2012) but also a limited role in conventional military operations, and the growing use by cyberspace by a wide variety of international actors.

CHARACTERISTICS AND THEORETICAL EFFECTS OF A NEW DOMAIN OF CONFLICT

Information Scarcity leads to Crisis Instability

The Internet is designed to be open, fast, and frictionless (Timburg, 2015), which has the unintended consequence of creating a domain of conflict whose primary characteristic is information scarcity and anonymity of actors. For example, while guns are fired by individuals with normally obvious allegiances and motives and ballistic missiles are fired from within well-defined sovereign borders, an aggressor's identity and the physical source of a hostile act in cyberspace are obfuscated with relative ease compared to traditional domains of conflict such as land, sea, and air. In fact, it is the only domain where the source of a large-scale hostile act is not immediately obvious. This problem of information scarcity has a number of strategic consequences.

Theoretically, cyberwarfare invalidates traditional models of deterrence. Deterrence is the use of the threat of unacceptable retaliation to avoid being attacked in the first place. Put simply, actors in cyberspace are able to "evade detection and disregard threat of retaliation" by properly hiding their identity, and so "deterrence loses its credibility" (Gartzke, Lindsay 2015). Traditional defense strategies employed by a number of powerful countries such as the United States, Russia, and China whose strategies are all more or less reliant on deterrence are invalidated. As countries slowly

adapt old strategies to a new reality, theoretically hostile actions in cyberspace will be handled with a strategy and doctrine that is inconsistent with the practical characteristics of reality; this can lead to consequences that benefit neither party in a conflict.

The information scarcity problem has the potential to cause misperception and crisis instability. Misperception, the situation in which one party misinterprets the motives, signals, or capabilities of adversaries, can lead to unintended and unfavorable actions, responses, and consequences for all those involved. Misinterpretations of these kinds can have massive consequences in crisis scenarios leading to unintended escalation of conflict between parties. In any domain of conflict, misinterpretation can lead to crisis escalation and an outright war that could have been avoided had perfect information about motive, identity, and capability been known to all parties.

In summary, the anonymity that the Internet creates new realities in which traditional models of defense are suboptimal and the lack of information can lead to crisis instability.

Information Scarcity Does Not Mean Information Deficiency nor Directly Causes Crisis Instability

Information scarcity does not necessarily mean that information that can be entirely hidden. It is reasonable that critical information, such as the identity of an aggressor, can be determined with reasonable confidence. In information scarce situations, while conclusive and exact information can rarely be determined, circumstantial evidence can more often than not provide adequate enough information for decision makers to make relatively informed conclusions about events and corresponding choices. For example, analysts could look at techniques, tactics, and procedures that provide evidence about the types of actors that use them. While the distinction should be made that circumstantial evidence and conclusions gleaned from it aren't as useful as conclusive information, it still helps decision makers in crisis scenarios; this decreases the chance of unintended escalation and miscalculation of the effects of hostile actions.

A good example of how identification can be done circumstantially is Stuxnet. To review, Stuxnet was an intrusion into the Natanz Nuclear Reactor in Iran in 2010 that ultimately destroyed approximately 1000 centrifuges and is estimated to have set back Iran's suspected nuclear program by approximately 2 years (Katz 2010). It is suspected that the United States and Israel worked together to develop, operate, and introduce Stuxnet into Natanz for the following reasons.

First of all, the virus was so sophisticated and the method of intrusion (which had to be physical because Natanz was airgapped (Zetter 2014), not connected to the

Internet) so complicated that only a well-resourced, persistent, dedicated, intelligent actor could have done it (Rid). Only powerful states have these kinds of capabilities and resources narrowing down our range of actors to approximately 20 countries. When we confine our scope to those of only states we can further narrow our range of actors to only countries with adversarial relations with Iran at the time; narrowing it down to a list that would approximately have the United States, Israel, Saudi Arabia, India, United Kingdom, and France. Now just because these countries have capability and motive does not mean that all of them developed Stuxnet. Finally we can look at the target that was attacked; the Natanz Nuclear Facility in Iran was suspected of being the primary research and development site for uranium enrichment for the creation of an Iranian nuclear weapon. Furthermore, both the United States and Israel are the countries on our previous list that have taken the hardest stance against the proliferation of weapons in the Middle East; a stance that has resulted in sanctions, military actions, and political campaigns against countries in the region such as Syria (2007 bombing of a suspected nuke plant) (Clarke, Knake) and Iraq (US invasion in 2003 based of justification of WMDs). While these reasons are not conclusive and provide no definitive answer of the perpetrator, the US and Israel are the only countries with the capability and fit the profile.

Predominance of Offense in Cyberspace Leads to Increased Frequency of Conflict

It is the common narrative in cybersecurity that the attackers naturally have an advantage over the defenders (Lynn). The vectors of attack into a networked system are numerous and sometimes unknown to the administrators of the network; defenders must protect against all threat vectors, known and unknown, while "the attacker only has to get in through one node just one time to potentially compromise all the defensive effort[s]" (Singer, Freidman 2014). In a more abstract sense, aggressors bear minimal costs and risks while defenders carry enormous costs and risks and still remain at a tactical disadvantage. Furthermore, as stated previously, because attackers can generally hide their identity, the risk of retaliation is minimal further reducing the barriers to entry for aggressors. In sum, cyberspace, as a domain of conflict, is considered to be an offensive dominant environment; this carries massive consequences according to prevailing theories of offense and defense in military confrontations.

Offense-Defense Theory and its underlying idea of "The Cult of the Offensive" (Van Evera 1984) states that in an environment where offense is dominant, conflict is, in general, more likely to take place; the opposite when defense is dominant. In the offensive dominant world, it is believed that the first strike will be the deciding one,

significantly magnifying perceived dangers and threats. In general this makes states, especially when they are unsure of the motives and capabilities of their adversaries, likely to carry out a preemptive strike, provoke conflict, or make the first strike in order to win a war that is believed to be inevitable; this increases the frequency of conflict. The example most often pointed out is that one of the underlying reasons that WW1 broke out is because world leaders at the time believed that, due to advances in military technology such as machine guns and airplanes, offense was advantaged and the first strike would be the only meaningful one (Van Evera). Furthermore, offensive dominant environments provide opportunities to revisionist states, rising powers that disrupt the status quo and will often take greater risks and are more likely to provoke conflict than well-established powers, to change international power structures in significant ways in their favor. Using the WW1 example, Germany was considered to be a rising power, defiant of the status quo while France and Britain were considered to be well established.

Applying Offense-Defense Theory and "The Cult of the Offensive" to conflict in cyberspace, it appears that the advent of cyberspace tips the scales in favor of the aggressor. Because the barriers to entry, such as development costs, and risk of retaliation, are so low and potential effects can be global and disruptive, cyberspace appeals to small, weak organizations; this is because they can credibly have the same capabilities and pose legitimate threats comparable established military powers.

Groups with a wide variety of motives, such as revisionist states, terrorist groups, organized crime, and even lone actors, can pose significant threats to status quo powers. In addition to this, well-established powers should be competing with these actors as well as each other with a higher frequency primarily in cyberspace; competition that certainly could break out into a more conventional war.

The dominance of offense in conflict in cyberspace has significant theoretical consequences that are potentially destabilizing to international order. It empowers previously weak actors with means to inflict damage on a scale that is global and disruptive.

Reasons why Cyberspace Does Not Produce the Effects of an Offensive Dominant Environment

Though some argue that cyberspace will ultimately not affect the nature nor frequency of conflict between small and large powers alike, it is simply not reflected in reality. Since the advent of the Internet and networking technology, formal wars between countries that originate in or include cyberspace as a significant characteristic of the conflict have never taken place. Furthermore, significant hostile events that do primarily involve cyberspace are not global and disruptive in scope, rather they are "restrained and regional" (Gartzke, Lindsay) in their effects. Examples include Stuxnet

which was limited primarily to Iran and did no damage to anything other than the Natanz Nuclear Reactor and the Sony hack which remained confined to a branch of a large corporation in the US and did not escalate hostilities between the US and North Korea. Both of these operations, characterizing examples of "cyberwarfare", are nothing more than covert operations limited in their goals, scope, and effects that fall far short of war. Because of this it appears that the utility of cyberspace remains primarily limited to covert operations (Rid).

Another aspect that alarmists do not consider are the sheer technical barriers to entry that preclude most actors from operating efficiently and significantly in cyberspace. Exploits that grant access to commonly used computer systems and software are difficult to find and therefore highly valued. Furthermore, once an exploit is used, it is generally patched by a network of highly skilled civil society experts within hours of its discovery by the public; this makes any vector of attack using that exploitation obsolete. Another point is that cyberweapons must be "designed" (Zetter) for a specific purpose and target in mind. In general, conventional weapons like guns and missiles are created without a specific target in mind. On the other hand cyberweapons must be specifically engineered and designed with the target, scope, and purpose specifically designed in. For example, the Stuxnet virus was designed specifically to destroy centrifuges at the Natanz Nuclear reactor. It could not be used to attack an American electrical general, another nuclear plant in Iran, or even damage

other systems in Natanz. This barrier significantly limits the practical utility of cyberweapons. Because exploits lose their usefulness when they are used and attacks must be designed for a very specific rather than a general purpose, cyberweapons are one-shot weapons that fire silver bullets.

The theory of how cyberwarfare is going to change the nature and frequency of conflict is not reflected in reality because traditionally dominant actors remain dominant and technical challenges make it difficult for any organization except for a well-resourced, intelligent, persistent actor to significantly affect power structures.

Lack of a Distinction Between an Act of War and Espionage

In Cyberspace, there is little difference between espionage, an act that is often limited in scope with minimal strategic consequences, and war, an act with large scope and consequences; while both are certainly hostile acts, they carry significantly different implications and responses (Kello 2013). Both Computer Network Exploitation (CNE), the realm of covert activity, and Computer Network Attack (CNA) (Zetter 2016), the realm of open conflict, use the same vectors of attack to gain access to the networks that hold an aggressor's objective. In most cases upon detection of an intrusion, the objectives of the aggressor are not immediately apparent to the victims until those

objectives are completed. Damage can be defined as anything from the exfiltration of sensitive information to the wholesale destruction of a networked system.

Similar to the problems of attribution and identification, the lack of distinction between war and espionage has the potential for crisis instability and escalation (Kello). For example, say a victim, State A, were to detect an advanced persistent threat in progress into a network that controlled a critical train transportation system, an intrusion State A can credibly identify as being perpetrated by State B. Also say that State B's motives are to gather information about what these trains are transporting, but this motive is not known to State A. State A would have no way of knowing if State B was attempting to disrupt State A's train schedules and rail systems or simply gain information that is under the purview of that transportation system. While gathering sensitive information is a hostile act, it certainly does not constitute an act of war whereas sabotaging an entire rail system certainly does (BBC). By itself, the presence of State B, in State A's critical computer networks tells State A nothing about the motives of State B. On the other hand, all it tells State A is that it is subject to a credible, vague, and potentially calamitous threat by State B; the worst case scenario being the destruction of a rail system critical to national security. State A, under the assumption it was under attack or about to be attacked, may retaliate against State B as if the two were at war with each other. While this example is hypothetical, this is a

misunderstanding that could easily take place in cyberspace that would lead to open war between states.

The lack of distinction between CNA and CNE, symptomatic of information scarcity, a characteristic problem of cyberspace, will cause misunderstandings between countries that will lead to war.

Similarities Between Acts Espionage and War Will not Lead to Crisis Instability

The major argument against this is that espionage is a norm between adversary countries. Because cyberspace has well proven utility for espionage and less proven utility for military operations at the moment, cyberspace as a domain of conflict has a stabilizing rather than a destabilizing effect. While this does not seem intuitive, generally espionage and information gathering efforts, although hostile, actually help create stability for the following reason.

Rivals on the international scale use espionage to gain a better understanding of each other's intentions, capabilities, and motives (Clarke, Knake); generally, availability of this type of information helps alleviate fears of imagined or overblown threats to security because it helps provide critical information to decision makers. Because of

this, it is understood that while espionage certainly constitutes a breach of sovereignty, espionage between rivals is an accepted international norm.

For example, most militarily advanced nations use satellites with cameras mounted on them to take pictures of each other's military installations. Despite the fact that these satellites can readily be shot down or rendered inoperable, as shown by China in 2007 (Gruss 2015), it has never yet happened that one country has shot down an adversary country's satellite (Clarke, Knake).

Another argument is that, similar to other arguments against alarmist theories, this has not been reflected in reality. Full scale military conflicts between states generally does not originate from covert activity both within and outside of cyberspace. For example, the downing of the U2 Spy Plane and the capture of American pilot Gary Powers, a famous example of the discovery of espionage by adversary state at the worst led to a deepening Cold War rivalries and further souring of already strained relations between the US and the Soviet Union. It was a boldly hostile act, far more hostile than any breach of sensitive information based in cyberspace, that did not lead to an outright war.

Cyberspace offers significant opportunities for espionage that states have readily exploited. Whereas its application outside of covert activity is somewhat limited and more conventional methods are used for activities such as naval conflict. Because of this, cyberspace is a bountiful source of information about the motives and

capabilities of potential adversaries; this produces a stabilizing effect rather than increasing the frequency of conflict.

Asymmetrical Warfare Potential in a New Domain

Cyberspace is a domain that is easily accessible. Technical barriers to entry to such as gaining the requisite knowledge and materials are often available commercially or for free to the public at large. Psychological barriers to entry such as the fear of retaliation or the fear of ineffectiveness are reduced by the anonymity of the internet and the offensive dominant nature of conflict in cyberspace, respectively. Ultimately this means that a very large number of persistent actors with a variety of motives, both state and nonstate, can freely enter and operate in this domain. This ultimately should empower revisionist powers, paramilitary and terrorist organizations, private corporations, activists, and lone actors to be able to use asymmetrical tactics against well-established powers to achieve their goals (Lynn) in ways that have not been available in traditional domains of conflict.

Asymmetrical warfare is a strategy that weak powers use against strong, well-established powers when the two are in conflict. Techniques, tactics, and procedures that characterize asymmetrical warfare are terrorism (suicide bombings of public spaces), subversion (attempting to undermining a government's authority by attacking

its economic institutions), guerilla tactics, surprise attacks, sabotage, and assassination. Asymmetrical warfare has been used throughout history. A variety of groups characterized throughout history as revolutionaries, rebels, freedom fighters, and terrorists such the FLN in Algeria, the Lehi in British occupied Palestine, revolutionaries in Britain's American colonies, Bolsheviks in Imperial Russia, Kurdish Separatists in Turkey, and Islamic State use asymmetric tactics against far more powerful countries.

Cyberspace, a domain that allows small actors to have the same global and disruptive effects as large actors, gives opportunities for these kinds of organizations to use asymmetrical warfare. For example, in Al-Qaeda's seven phases for achieving its strategic goals, it references the employment of cyber warfare to attack the US's economic institutions and undermine trust in the American economy in the fourth phase (Musharbash 2005).

Also, in some ways, weaker powers are actually advantaged in cyberspace because they generally do not have underlying digital systems that control critical infrastructure whereas strong state powers generally do. Status quo powers such as the United States are, in this sense, disadvantaged compared to weak powers due to their reliance on vulnerable digital systems. Weak powers need not fear a proportional response in cyberspace to provocation, simply because there are comparatively fewer, if any, digital systems that the weak power is reliant on.

Because of the low barriers to entry, high potential for effectiveness, and low risk of unacceptable retaliation, many previously disenfranchised, nontraditional actors can enter the domain and produce globally disruptive effects threatening the national security of traditional powers.

Cyberspace Affords Greater Opportunity to Stronger Powers than Weak Powers

Alarmists argue that because cyberspace is an offensive dominant domain in which weak powers can easily hide from strong ones and have similar capabilities as strong powers, it should empower disenfranchised actors who will provoke conflict and change the status quo. In reality, traditionally dominant military powers are the ones who are also dominant in cyberspace (Gartzke). While other actors both state, like Iran or North Korea, and nonstate, like Islamic State or Anonymous remain active, their power in cyberspace is significantly limited in the same ways their capabilities in more conventional military domains are limited. It is traditionally powerful states such as the US, Russia, and China that are the most sophisticated and the most active in cyberspace.

This is certainly not to say that smaller powers are not active in cyberspace. There have been countless cases of the use of cyberspace by smaller actors against larger ones. However, these provocations are generally limited in scope and technical sophistication compared to those committed by powerful countries. For example North Korea's attacks on Sony, Iran's attacks on corporations owned by Sheldon Adelson, and Islamic State's defacement of websites under the dot mil domain are, at best, high profile acts of vandalism or limited attempts at subversion. These actions are small compared to the scope, scale, and sophistication of the US's Operation Olympic Games, Russia's large scale compromise of US military networks known as Moonlight Maze, or China's suspected compromise of a large number of western diplomatic institutions known as GhostNet (Kaplan); acts that range from large scale espionage, sabotage, and by some measures, very serious and significant breaches of sovereignty.

Just like any other domain of conflict, small powers will operate and exist but traditional powers will dominate.

US SPECIFIC ISSUES IN CYBERSECURITY

Critical Infrastructure

The term "critical infrastructure" was an idea introduced in the Obama administration in PPD-21 to centralize national security efforts. It is defined as the

pieces of "infrastructure sectors whose assets, systems, and networks, whether physical or virtual, are considered 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" (Department of Homeland Security). Examples of critical infrastructure include the electrical grid, the water supply, and transportation systems.

A significant portion of critical infrastructure in the United States is owned by private industry. For example nearly 3/4ths of US electrical power is supplied by the private sector (Kello). Because market forces dictate the priorities of these companies and security would increase operating costs while not increasing the value of its products to its consumers. This has ultimately led to the situation where owners of critical infrastructure are, as Richard Clarke described, spending "more on coffee than IT security" (Clarke). As of right now there is a market inefficiency that ultimately creates significant vulnerabilities in infrastructure that the US itself defines as necessary to its national security.

Opposition to Regulation by the Private Sector and Civil Society

Regulation regarding cybersecurity has a fairly unique history in the United States. It is an issue in which private industry and civil society, two parts of American

society that generally disagree even on issues of general governance of the Internet, actually have a similar stance about cybersecurity regulation; albeit for significantly different motives.

As stated before, opposition from the private sector comes from the fact that increased investment into the digital security of products is a cost that affects the bottom line of American corporations. Especially in the fast paced environment of the US technology sector, which is characterized by significant economic incentives for being first to market, releasing minimum viable products quickly, and generally fast-paced development cycles, cybersecurity may become a lower priority. The private sector opposes regulation requiring cybersecurity practices to be adhered to, arguing that more regulation discourages innovation by raising barriers to entry, such as costs and gaps in specific areas of knowledge in programming and computer science.

Opposition by civil society, groups that seek agendas that promote certain causes (examples in of civil society in the US include a wide variety of groups from the National Rifle Association to the American Civil Liberties Union), comes from the fact that regulation generally comes at the cost of individual privacy and liberties. Regulation that seeks to increase the security of digital systems requires empowering law enforcement and access to sensitive personally identifiable information as a condition for the use of internet services. Civil society has generally pointed out that,

while these regulations do increase security, they take away from privacy and such access and information could easily be abused to crack down on freedom of speech.

Another significant point that civil society brings up is that the US is considered, internationally, to be a standard setter for human rights such as privacy and freedom of speech; if the US were to institute regulations that have the potential to be used to stifle political dissent, other countries with far worse human rights records and standards could use US laws and standards as justification for their own very real human rights abuses (Khamooshi, 2016). Ultimately, civil society opposes cybersecurity regulation because, although it increases security, it comes at the cost of constitutionally guaranteed rights.

These two issues can be defined generally as a problem of regulation versus the free market and regulation versus civil liberty, respectively.

Failed Attempts at Regulation by the US Government

One example of the failure of cybersecurity regulation in the early days of the Internet and networked systems was the Clipper Chip controversy that took place in the 90s. The clipper chip was a device invented by the NSA that encrypted data on cellular devices that contained a backdoor that could by law enforcement (Levy 1994).

The proposal was to install these chips onto all cellular devices to make ensure the privacy and security of sensitive private information of US citizens. The proposal was widely refuted by the private sector as well as civil society for a number of reasons. As for the private sector the refutation was fairly straightforward; requiring private companies to work with the NSA to manufacture, maintain, and engineer compatibility with clipper chips with their own devices imposed unnecessary costs on cellular providers and manufacturers. As for civil society, the response was more nuanced. While, in theory, a device that ensured the security of private information developed by the world's leading cryptologists and security engineers should be favored by civil society, the development of a backdoor that could bypass all security measures was impossible to accept and invalidated any theoretical gains in security. This is because, the US government or one its agents could easily overstep their authority and spy on private citizens arbitrarily and without warrant. Secondly, from a security perspective while the installation of a backdoor to an accountable, trusted individual or institution is by itself not a bad thing, the same backdoor could necessarily be discovered by a malicious organization or individual; backdoors themselves actually hobble security in such a way that it completely invalidates any benefits that backdoor provides. In the end, the clipper chip proposal was completely rejected by the American public.

A more contemporary example along similar lines, is the short debate over encryption after issues in the investigation by the FBI following the San Bernardino

shootings and a legal battle between the investigators and Apple Inc. During the investigation, Apple refused to help the FBI break into an iPhone owned by one of the shooters because they said it will compromise the security of all iPhones, a popular consumer product, and set an unfavorable legal precedent (Khamooshi).

Proposals came from Congress (Burr-Feinstein Bill), particularly Senators Richard Burr and Diane Feinstein (Conger 2016), which would have compelled organizations such as Apple to weaken their security measures on their devices to give access to encrypted data on devices. Once again the private sector, led by Apple, took a strong stance against these proposals, as it would reduce efficiency, due to the fact that devices would need to implement two computationally costly encryption standards, and effectiveness, because one of those encryption standards would be designed to be broken. These revisions would ultimately make products more costly, lower quality, and overall less attractive to consumers. Civil society brought similar arguments about backdoors to the encryption debate that were brought to the clipper chip controversy. Additionally, civil society argued that, because Apple is a multinational organization whose products are widely used in a variety of countries with differing human rights records and standards, other countries would readily request access to this backdoor under the same legitimate justification law enforcement. For example, China, a major market for Apple products, could request access to encrypted data on a iPhone of a suspected political dissident which Apple would be compelled to accept. The

proposals were quickly tabled and Apple retained the right to refuse granting access to personal data on its products.

Ultimately what these examples show is not the inability to enact significant cybersecurity reform, more these are exemplary of how government has generally failed to implement reforms that take into account the needs of private industry and civil society.

CASE STUDIES

Stuxnet

As technology further advances, it can also become more vulnerable as we see in the case of Stuxnet, a computer virus that was first detected in June 2010. It was the first time a piece of computer malware was detected that was able to attack industrial operations.

Within a month of its discovery, Liam O'Murchu, an analyst for Symantec Corp., a large antivirus company, was trying to determine what this virus was trying to accomplish—not an easy task since it was tens of thousands of incredibly complicated

and sophisticated lines of code, that had flown under the radar for about a year until its discovery.

What made this virus different compared to others of its kind was that it was not trying to steal passwords, or identities, or money which were common targets of viruses at the time. Instead, it was systematically weaving its way through the computers to find industrial operation Siemens Programmable Logic Controllers (PLC) which are used in factories all around the world regulating everything from traffic lights, to assembly lines, to oil and gas pipelines, and nuclear power plants (Stuxnet: Computer Worm Opens New Era of Warfare). Unlike other viruses, it didn't have to forge a security clearance; Stuxnet had a real security clearance, allowing it to bypass any of the implemented protection features (Stuxnet - Anatomy of a Computer Virus). Furthermore, since it was spread over USB drives instead of over the internet, it was easier for the virus to remain hidden (Stuxnet - Anatomy of a Computer Virus). Needless to say, the virus was highly sophisticated compared to other contemporary malware.

Though the virus was discovered, its ultimate goal was not known. After monitoring the virus, it was found that its information was sent to two untraceable websites in Denmark and Malaysia (Stuxnet: Computer Worm Opens New Era of Warfare). However, with reverse engineering it was found that most of the affected sites were in Iran. This led to the realization that this virus didn't attack every computer

it affected; there was one specific target: a factory floor of the Natanz Nuclear Plant in Iran with unique equipment and centrifuges used to enrich Uranium, an integral part in the creation of nuclear weapons (Kushner). The virus was designed for the centrifuges to start spinning faster and essentially self-destruct so the uranium was damaged and unusable, all while preventing operators from seeing anything was wrong (Kushner).

The United Nations' International Atomic Energy Agency filed a report saying that a thousand to two thousand centrifuges were removed from the power plant for "unknown reasons," meaning that Stuxnet succeeded in its mission to damage the centrifuges enough keep Iran from advancing its nuclear weaponry plan (Nakashima).

The discovery of Stuxnet led to serious considerations about the consequences that cyber warfare can have on the world. This is the first weapon to be created entirely out of code and it's clear that cyber weaponry cannot be destroyed (Weinberger). In fact, the full code is available for anyone to download and reconstruct to further one's own agenda, and it's unknown just how deleterious its effects can be (Stuxnet: Computer Worm Opens New Era of Warfare). Even O'Murchu stated "We [engineers] look at code [but] this was the first real threat we've seen where it had real-world political ramifications. That was something we had to come to terms with (Kushner)." It's been stated multiple times that the "third world war" would be fought in the cyberspace, but how far could it go? If hackers are able to team up to take down a

highly secured nuclear power plant with a worm that went unnoticed for a year, then who knows what other infrastructures could be attacked?

Currently the power plants and critical infrastructure our world runs on are privately owned and vulnerable (Ashford). Senator Collins stated, " I cannot think of another area [in Homeland Security] where the threat is greater and we've done less. We cannot afford to wait for a 'cyber 9/11' before taking action ("Experts Predict Future Homeland Security Threats")." Cyber warfare could permanently damage everyday parts of our lives.

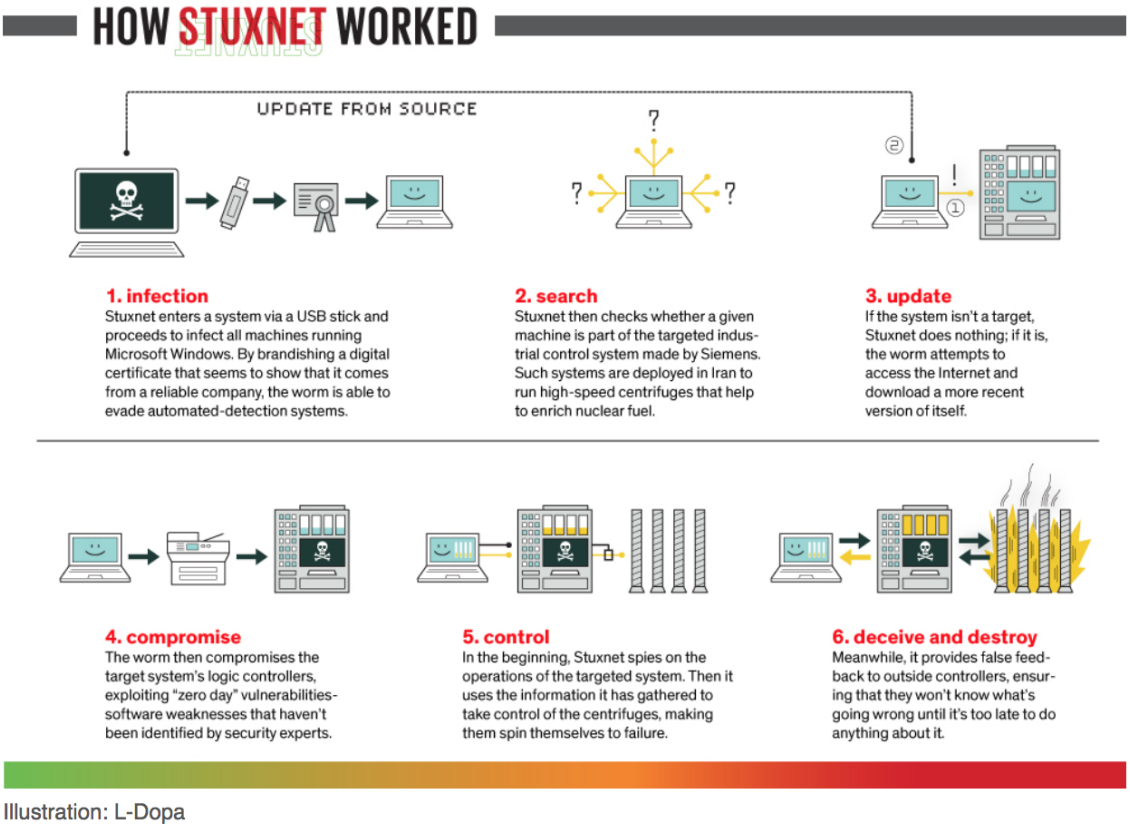

Figure 1: *Diagram explaining Stuxnet mechanism*

QUESTIONS TO CONSIDER

1. In your opinion, what are the implications of characteristics unique to cyberspace?
2. Where should the line by drawn between an act of espionage and an act of war? How should the US respond to each act? Are there instances that set historical precedent?
3. What are some examples of shortcomings in US national security strategy in cybersecurity?
4. How has the US arbitrated between opposing stakeholders in cyberspace such as national security and the private sector?

Works Cited

Ashford, Warwick. "Most Nuclear Plants Not Prepared for Cyber Attack, Says Chatham House." ComputerWeekly. Computer Weekly, 5 Oct. 2015. Web. 19 Aug. 2017.

BBC. "GCSE Bitesize: Manchuria." BBC. BBC, n.d. Web. 29 July 2017.

Clarke, Richard A., and Robert K. Knake. Cyber War: What It Is and How to Fight It. New York: Ecco, 2010. Print.

Clarke, Richard. "A Quote by Richard Clarke." Goodreads. Goodreads, n.d. Web. 29 July 2017.

Conger, Kate. "Burr-Feinstein Encryption Bill Is Officially Here in All Its Scary Glory." Tech Crunch 13 Apr. 2016: n. pag. Web. 28 July 2017.

Department of Homeland Security. "Critical Infrastructure Sectors." Critical Infrastructure Sectors | Homeland Security. Department of Homeland Security, n.d. Web. 29 July 2017.

Evera, Stephen Van. "The Cult of the Offensive and the Origins of the First World War." International Security 9.1 (1984): 58. Web.

"Experts Predict Future Homeland Security Threats." Homeland Security & Governmental Affair Committee. United States Senate Committee, 11 July 2012. Web. 20 Aug. 2017.

Gartzke, Erik, and Jon R. Lindsay. "Weaving Tangled Webs: Offense, Defense, and Deception in Cyberspace." Security Studies 24.2 (2015): 316-48. Web. 28 July 2017.

Gartzke, Erik. "The Myth of Cyberwar: Bringing War in Cyberspace Back Down to Earth." International Security 38.2 (2013): 41-73. Web.

Gruss, Mike. "Pentagon Says 2013 Chinese Launch May Have Tested Antisatellite Technology." SpaceNews.com. Space News, 14 May 2015. Web. 29 July 2017.

History.com Staff. "U-2 Spy Incident." History.com. A&E Television Networks, 2009. Web. 29 July 2017.

Kaplan, Fred. Dark Territory. Place of Publication Not Identified: Simon & Schuster, 2017. Print.

Katz, Yaakov. "Stuxnet Virus Set Back Iran's Nuclear Program by 2 Years." Jerusalem Post 15 Dec. 2010: n. pag. Print.

Kello, Lucas. "The Meaning of the Cyber Revolution: Perils to Theory and Statecraft." International Security 38.2 (2013): 7-40. Web.

Khamooshi, Arash. "Breaking Down Apple's IPhone Fight With the U.S. Government." New York Times [New York City, New York] 21 Mar. 2016: n. pag. Print.

Kushner, David. "The Real Story of Stuxnet." IEEE Spectrum: Technology, Engineering, and Science News. IEEE Spectrum, 26 Feb. 2013. Web. 19 Aug. 2017.

Levy, Stephen. "Battle of the Clipper Chip." New York Times [New York City, New York] 12 July 1994: n. pag. Print.

Lockheed Martin. "Cyber Kill Chain." Cyber Kill Chain® · Lockheed Martin. Lockheed Martin, n.d. Web. 28 July 2017.

Lynn, William, III. "Defending a New Domain: The Pentagon's Cyberstrategy." (n.d.): n. pag. Cyberwar Resources Guide. Web. 28 July 2017.

Murphy, Matt. "War in the Fifth Domain." The Economist 1 July 2010: n. pag. Print.

Musharbash, Yassin. "The Future of Terrorism: What Al-Qaida Really Wants - SPIEGEL ONLINE - International." SPIEGEL ONLINE. SPIEGEL ONLINE, 12 Aug. 2005. Web. 29 July 2017.

Nakashima, Ellen. "Stuxnet Was Work of U.S. and Israeli Experts, Officials Say." The Washington Post, WP Company, 2 June 2012. Web. 18 Aug. 2017.

Naraine, Ryan. "Stuxnet Attackers Used 4 Windows Zero-day Exploits." ZDNet. ZDNet, 04 Dec. 2015. Web. 18 Aug. 2017.

National Archives and Records Administration. "The Zimmermann Telegram." National Archives and Records Administration. National Archives and Records Administration, n.d. Web. 28 July 2017.

Rid, Thomas. "Cyber War Will Not Take Place." Journal of Strategic Studies 35.1 (2012): 5-32. Web. 28 July 2017.

Ryan, Jason. "CIA Director Leon Panetta Warns of Possible Cyber-Pearl Harbor." ABC News [New York City, New York] 11 Feb. 2011: n. pag. Print.

Singer, P. W. "Cult of the Cyber Offensive." Foreign Policy 15 Jan. 2014: n. pag. Web. 28 July 2017.

Stoll, Clifford. The Cuckoo's Egg: Tracking a Spy through the Maze of Computer Espionage. New York: Pocket, 2005. Print.

Stuxnet - Anatomy of a Computer Virus. YouTube. Spice Works, 25 Sept. 2015. Web. 20 Aug. 2017.

Stuxnet: Computer Worm Opens New Era of Warfare. YouTube. CBS News, 4 Mar. 2012. Web. 19 Aug. 2017.

USAF College of Aerospace Doctrine, Research and Educ Ation (CADRE). Three Levels of War. USAF College of Aerospace Doctrine, Research and Educ Ation (CADRE). Air University Press, n.d. Web. 28 July 2017.

Washington Post. "The Real Story of How the Internet Became so Vulnerable." The Washington Post. WP Company, n.d. Web. 28 July 2017.

Weinberger, Sharon. "Computer Security: Is This the Start of Cyberwarfare?" Nature Publishing Group. Nature International Weekly Journal of Sazcience, 08 June 2011. Web. 20 Aug. 2017.

Zetter, Kim. "Hacker Lexicon: What Are CNE and CNA?" Wired n.d.: n. pag. Web. 28 July 2017.

Zetter, Kim. "Hacker Lexicon: What Is an Air Gap?" Wired 12 Aug. 2014: n. pag. Web.

Zetter, Kim. "An Unprecedented Look at Stuxnet, the World's First Digital Weapon." Wired 11 Mar. 2014: n. pag. Web. 28 July 2017.

Zetter, Kim. "An Unprecedented Look at Stuxnet, the World's First Digital Weapon." Wired 4 Nov. 2014: n. pag. Web.

Image Sources

Figure 1: https://www.cyber.nj.gov/threat-profiles/ics-malware-variants/stuxnet