How Information and Communication Security Technologies Affect State Power

Joshua M. Campbell

Adviser: Scott Waalkes, PhD

Submitted in Partial Fulfillment of the Requirements for Graduation from the Malone University Honors Program

22 April 2016

Information and Communication Technology (ICT) is everywhere. It is impossible to go anywhere without seeing someone on their phone, tablet, or laptop doing anything from playing games to reading the news to working on a project. The seeming omnipresence of technology has made it easier for people to keep in touch with each other. However, the use of digital methods to keep in touch has made it easier to be tracked by both corporations who want people to buy their products or services and larger governments who want to keep an eye on the people who may be planning crimes of varying sorts.

While surveillance mechanisms have existed for an extremely long time, modern, ICT-based systems have come under the microscope. Recently, the far-reaching scope of the US Government surveillance system was exposed by the leaks of former government contractor Edward Snowden. Partly as a result of the transparency forced by Snowden, academics and journalists have recently engaged in a lively debate about the impact of ICT on governments around the world. In general we can organize the major contentions in this debate into three schools: the Centralization school, the Skepticism school and the Diffusion school. The centralization school points to the information released by Snowden, and its advocates argue that ICT allows government intelligence services to control far too much information, which increases large state power. Skeptics argue that technology's impact on world affairs has been overplayed. Proponents of Diffusion argue that ICT's proliferation makes it easier for smaller governments and non-state actors to network independently in cyberspace, free of the normal government controls that are tied to territory.

In order to discern which of these ideas is the most accurate, this paper will first look at each contention in more detail and some of the specific arguments their proponents make. Then, we will look at which contentions seem the most applicable. After that, we will look at several case studies to understand the strongest contention in detail before finally coming to some conclusions.

Characteristics of Modern ICT Systems

In order to better understand the impact of ICT on governments, this section of the paper employs Crouch's (2008) questions for diagnosing culture: What does the internet assume about the way the world is? What does the internet assume about the way the world should be? What does the internet make possible and what does it make impossible or difficult? And what new forms of culture are created in response to the internet? The rapid growth and adaptation of the internet by society makes it a very interesting cultural phenomenon, one that has transcended geographic borders to become global in nature. This growth is fascinating and begs the question of why? This section, looking at the internet as a cultural artifact, helps us to understand that partly.

The most integral part of modern ICT is the internet. Part of what makes the internet such an interesting phenomenon is how it integrated into the world. In the last quarter of the 20th century, university and government researchers came together to develop a system by which they could communicate more rapidly the findings of their research and to facilitate cooperation. From this basic transmission framework that would be akin to a much more basic version of e-mail, the foundations of the Internet was born. At this point, however, the network was barely more than a few end systems that could send and receive messages, and the cables that connected them to each other. As the century started to come to a close, the next iteration of the internet, a more familiar one, would begin to take form in what was known as the World Wide Web: the system of interconnected servers hosting websites, the content on those sites, the various files users can access and the cables connecting it all together.

What the Internet assumes about the way the world is

Still at the foundation of this entire system, though, is an underlying assumption that the world wants to communicate detailed information faster than ever before. Without the desires of researchers to be able to transmit their findings in minutes rather than days, the framework for the internet might not exist as it does today; the system would probably still develop, but later on as businesses thought about faster ways to interact with customers from home in collaboration with scientists understanding how technology works.

What the Internet assumes about the way the world should be

In addition, the internet includes in its underlying assumption that all information and people should be treated the same way. Early development of internet technologies involved dedicating an entire circuit to a given connection rather than the more modern way by which we package information up with an address, similar to physical mail, and send it to the next major node on the network where it gets sent on further. No matter if this is a heartfelt message of love from a wife to her husband overseas in the military, a malicious virus traveling in an e-mail or someone's shopping order, the internet does not make evaluations regarding who sends and receives the message nor what is in the message itself, it merely just passes it along.

What the Internet makes possible

This structure of equality of traffic is partly dependent on semi-anonymity within the internet and is what empowers groups like Anonymous to take action without as much fear of repercussion. The actions they take, like releasing Donald Trump's personally identifying information, or PII, or taking down websites, constitute a form of electronic vandalism. While not directly damaging to the interests of an actor, they typically force the victim to allocate extra resources to repair the damage done and may have lasting consequences. In the case of Trump, his information is now circulating around the internet and while some system administrators may attempt to remove this data from their servers, others take the principle of equality to heart and allow the information to remain on their servers. Trump may pay people to try and force web sites to take down his information. In the case of a downed website, this can result in a small public relations crisis where users are unable to access a given server which prevents their intended interaction with the site and, by extension, the entity that the site is about. The entity or their web host then has to spend extra time and money to restore the server to normal operation as well as suffer from the lost business due to the outage.

This is part of the reason why some hacker-vandals engage in Denial of Service, or DoS, attacks. One major style of DoS involves a hacker taking partial control over several other computers turning them into "slaves". Once setup, the hacker then commands all of the slaves to try to connect to the same web server. While servers can usually handle a good number of requests in an interval, the nature of the network infrastructure means that any server has a limited amount of resources. A DoS attack stretches these resources to a breaking point such that legitimate traffic is unable to access the site, as the malicious traffic will typically either take up all of the bandwidth, the amount of data a connection can service per time interval, the queue, the memory where web data packet wait until they are able to be processed which results in dropped packets when full, or the processing power, the power of the computer to do operations.

What the Internet makes impossible or difficult

A logical consequence of the speed of the internet is that it does not allow for much in the way of personal privacy. This occurs significantly in how human behaviors relate to the internet. Regarding human behavior and the internet, a society that is well connected to the internet typically allows for individuals who are witness to a significant event to bring up this event and spread it quickly. While this has more positive implications as it can warn people about a potentially dangerous or bothersome situation and helps them to stay away, more often than not this results in people sharing seemingly innocuous posts about their daily lives which may harm the livelihood of someone involved in the post. As an example, some people call in sick to work in order to take a day off. However, they then proceed to travel somewhere and post about their travels on social media. If they have their immediate supervisor on the given media, this could result in them losing their job. This also has contributed to how the paparazzi work in a similar regard, where one will take a photo of a celebrity in a situation and post it all over social media in hopes of it spreading across varying people's networks.

What new forms of culture did the Internet spawn?

The creation of the internet resulted in the creation of other major web services, such as e-commerce applications where consumers can proceed to do some of their shopping from their homes with an instant submission of the order. Services like Amazon allow for consumers to purchase products at a speed that is much faster than catalog ordering, its conceptual ancestor, allowed for and also allows consumers to find products that might otherwise be inaccessible such as local products from abroad or more obscure instances of generic products like movies or games. The internet also created new means of collaboration and connection. Social media services like Facebook allow for people all over the world who only have loose connections to a common idea, like mutual admiration of a person, to unite and interact with each other. For more productive means, people can now work simultaneously on a project miles apart with all changes being made available immediately to those looking at the project.

One other major by-product of the internet is mobile ICT. While mobile phones have been around for a few decades, the only communication they allowed for was voice-based. Similarly, computers were mostly stationary machines that had to be plugged in and connected to any device they wanted to interact with. The development of the modern internet has allowed for devices like laptops and smartphones which are both significant elements of ICT in existence and relatively recent developments. While laptops have been in play for the past 10-15 years, they still were based on a semi-developed internet, and smartphones are less than a decade old. While they are more a direct result of the innovations surrounding wireless internet, the internet is still a foundational element. Interestingly, a number of the developments of the current internet, including things like social media, are consequences of the mobile ICT developments.

While sites like Facebook and Twitter predate modern smartphones, they still had some minor interfacing with “dumb” phones. However, the features of Facebook during that time were very limited. Games were not as ubiquitous as they are now, and the idea of outside programs using social media accounts as a log-in mechanism was inconceivable. Smartphones, however, allowed users to interact with social media very easily from anywhere that they had a signal due to the growing mobile internet service. With the systems becoming easier to use, more people would create accounts that would give developers a bigger market to sell their products to. Thus, the growth of users would be the likely spawn of several games from more classic games like FarmVille to newer ones like the Saga family of games. Without mobile ICT, however, these games may not have ever come about as the user base may not have ever appeared.

Underlying any given modern ICT system is some sort of security mechanism. One reason for these security mechanism is the growing use of personalized aspects of the technological life which are kept behind a digital "lock" of sorts through passwords. While, in some cases, these passwords prevent people from accessing menial things such as social media and digital community accounts like Facebook or reddit, several implementations of password-protected systems can help secure e-commerce or other more vital applications where a lack of security could leak key information about bank accounts that could then be breached and its contents stolen. Thus, password-protected systems are a vital aspect to the security design for the internet.

However, any sort of system by which a password would be transmitted also needs to be protected in its own right. Someone using a key to unlock a vault doesn't want someone to have access to the key's shape as that would allow them to make a duplicate and thus gain unauthorized access to the vault. Thus, computer scientists have developed new tools for protecting information stored in a given location but also as it is in transmission. Any sort of what I will call a "Digital Information Security Technology" (DIST) is a mechanism by which such digital information can be encrypted and protected in such a way that only another person with the decryption information is able to remove the protection measures. This could include storing information on a computer where the password triggers the decryption or a system by which the data is encrypted, transmitted, and decrypted automatically when it reaches its target.

One example of a DIST is the RSA cryptosystem embedded into all modern web browsers. RSA uses a system of “public keys” and “private keys” to allow for the encryption of data as it needs to be transmitted and is founded upon the a principle that the product of two prime numbers of a large enough size is difficult to factor, even for a computer and especially for humans. By using the product and the choice of a pair of special numbers which meet certain criteria regarding modular arithmetic and exponents in combination with the product, RSA provides a secure means by which to protect data. A user, who we will call Bob, that wishes to transmit information to another user, Alice, can put that information into the formula that breaks down the digital version of that information into blocks and raises each block to Alice’s public key in modular arithmetic based on her product. This information is then transmitted publically over the internet. Note that if another user, Catherine, were to try and grab this data and interpret it, it would appear as a pile of gibberish. When Alice receives this information, she applies her private key in the same way Bob applied her public key, which results in Alice’s computer receiving the original message, which it then interprets to create the human-readable equivalent that Bob wanted Alice to see. This piece of DIST, while extremely common, has yet to be broken by any major means. The strength of this algorithm is what made it so popular. With this understanding of technology, though, it is now important to consider how this technology interacts with the state.

What is the Impact of ICT on State Power? Three Perspectives

School One - Centralization

This school focuses on the ideas that the U.S. government has a controlling interest on power and information in the current state of affairs, and this degree of control has made the U.S. the most central entity in terms of information usage. Many scholars used the leaked reports by former security analyst Edward Snowden in their discussion and eventual criticism of this model. Most of the criticism does not dispute that the U.S. government gorges on information; they only question the degree to which it does and how it matters. The standard operating procedure for the NSA, Centralization scholars generally note, is to function as some trawl fishermen do: throw their "net" into the ocean of information that is the internet and collect everything they possibly can while sorting out what is and is not useful once everything is collected. Even then, the information that lacks immediate use or is encrypted still is hoarded until such a time comes that it proves useful or can be accessed. Clearly, the focus in this school is on the current power focus in the U.S., in contrast to the Diffusion model's focus on non-state power. The general warning posed by Centralization scholars is one to ordinary people of caution and vigilance when on the internet, the government will see what you are doing.

Edward Snowden's work in leaking how the NSA operates forms a part of the foundation for Centralization. Many of these scholars use Snowden's work as part of their negative stance towards these highly pervasive surveillance systems. Using the leaking of confidential NSA documents by former National Security Agency analyst Edward Snowden, journalist Glenn Greenwald (2014) argues against excessive use of technology by the US government in their surveillance efforts in the post 9/11 landscape.

His book goes into a high degree of detail to describe everything that the NSA did in their standard operations of surveillance, including gathering information on billions of e-mails and phone calls in just one quarter. Through his book, Greenwald shows the excessive and potentially illegal amounts of intelligence gathering done. Greenwald's arguments are rooted in very similar arguments to those promoted by professor of international affairs Dr. Robert Dover's (2014) through their common example.

In issues of intelligence, the U.S. government did not exclusively focus on domestic targets. The notable case of the hacking of German Chancellor Angela Merkel shows an even more extreme degree to this system. In his article, Robert Dover uses the case studies of both Edward Snowden, similar to Greenwald, and Angela Merkel in his argument against an increase in technology usage in espionage. By looking at responses to both, Dover attempts to critique the US intelligence gathering services and the extremes that these services went to in their surveillance. Dover also discusses the implications that these scandals had on the internet at large and its decentralization.

While the work that Snowden did to help reveal the U.S. surveillance system forms a solid base, generalizing these ideas of how governments engage in espionage and surveillance is just as important. David Tucker (2014) presents a modern look on intelligence gathering. Though his analysis does not include any major case studies, Tucker demonstrates what modern intelligence looks like and the implications it has for the future through philosophical and legal perspectives in light of modern technology with minor examples played through long-term examples of two spies compared to case studies as Greenwald and Dover do. In particular, he notes implicitly the need for a better legal structure to match the technical systems in place now.

Modern big businesses are also entering into the surveillance community under the related field known as “Big Data”, or demographic data collected for purposes such as marketing. While their motivations are different than those of the government, the fact that companies are collecting data with the potential to sell this data to other companies or even the government shows how integral data collection practices have become. By looking at the industrial side of technical offerings, journalist Robert O’Harrow (2006) scrutinizes the amount of technology being used to gather intelligence by not only the government but many other companies such as rental car companies. O’Harrow takes the middle ground between the case studies of Dover and Greenwald and the more theoretical approach taken by Tucker by looking at small, numerous examples of companies using electronic surveillance and other forms of ICT to track people through the massive amounts of data collection being done. His analysis follows a similar line of logic to Dover, where he focuses on the negative impacts that this persistent surveillance has on society.

Americans tend to espouse their country as the paragon of freedom and democracy in contrast to authoritarian countries where dissent is frequently met with government intervention. However, the combination of the surveillance technologies being used by these authoritarian powers and the system already in place in the U.S. demonstrates how the U.S. might seem in a short time. While Brookings Institute scholar John Villasenor (2011) focuses mostly on the surveillance states created by authoritarian regimes, his arguments heavily relate to what could become the future of the United States. By looking at how authoritarian governments surveil their own people in terms of hardware and supplementary tools like encryption, Villasenor notes how foreign governments will be able to use ICT and related media like Facebook and camera footage to track down dissidents and eliminate threats. While this does cause issues for the U.S. government in terms of foreign policy matters, it also demonstrates what power the government might be able to have when it combines its massive catch-all database with other systems.

While many of these scholars have different specific messages, their overall theme is the same; the largest global governments, such as China, the U.S. and Russia, have obtained a vast amount of information on its citizens and even foreign nationals, and the practices used to collect this data need to come to an end. None of these scholars suggest a continuation of these practices, not even in the oft-cited reason of "National Security." Unfortunately, the cessation of these surveillance practices are unlikely, given the lack of accountability to the public that the government intelligence services have, as evidenced by the surprising nature of Snowden's revelations (Greenwald, 2014).

Some statisticians warn against extrapolating from existing data using the example of trying to predict the height of young adults using the childhood growth rates. While a pattern may be true at a specific point, the continuation of that pattern is not guaranteed. Likewise, while the existing relationship between ICT and government seems to be one that promotes centralization, the public's backlash against the surveillance programs and their efforts to try and stop, or at least stagger, them seems to indicate that this model will not be as good of a predictor as the ideas in the Diffusion school.

School Two – Skepticism

Skeptics hold that the impact of technology is being overplayed. While the cyber domain still needs to be considered, the physical states and all that they represent are a more important consideration in modern political system. Territory still matters. Laws continue to be enforced within sovereign states by governments whose writ is limited to their clearly defined territories. While technology augments the structures already in place, they are still significantly dependent on the physical structures that governments currently control and manage. For example, the "cloud" server systems which holds data on the internet have physical addresses in physical buildings requiring electricity and physical security. As a result, the impact that technology has had on non-state actors being involved is, according skeptics, being overplayed. What we call the cloud may be better referred to as the fog due to ground-based presence.

One very notable skeptic is Evgeny Morozov, who wrote in his book (2011) that the effectiveness of technology in protests like the 2009 Iranian Revolution was overplayed by the western media. The fast acceptance of technology into modern culture has been an overall negative for society, according to Morozov. One of his main points is that by governments too lightly accepting the role of technology into society, it tacitly precludes other options for what direction policies should go. It also causes them to see many technical tools politicized such as blogging platforms.

While technology is everywhere, there are still very physical limitations to what it can do. Martin Wolf, a journalist for *Foreign Affairs*, wrote in an article (2001) that the physical anchors of government and society like the economy are what will keep technology from completely taking over in the modern globalized society. In addition, he sees no difference between modern trends towards technical transmission of information and their older analogs. By developing proper policies, according to Wolf, technology's impact can be diminished. In general, the states still control large amounts of power and technology has not significantly changed that.

These physical limitations also exist in that modern technology requires significant amounts of community developments in order to properly function. In an article he wrote for the Army magazine *Parameters*, Martin Van Creveld (1996) argues that technology would not be where it is now without the state to help guide it. The systemic nature of systems like the internet and telecommunications requires that someone pay to provide the infrastructure; the cables, servers and transitional nodes that serve as the physical layer for the internet; that allows these systems to function. As governments are really the only groups with the capital to make them function well, we would not be seeing the current technical state without the physical state to support it. Beyond the individual states helping foster technological growth, international cooperation is crucial in understanding how the internet is so prolific today. Without a degree of cooperation, most countries would setup their own domestic networks and not link them together with others. This leads to problems if you are trying to work with someone abroad and e-mail or online storage solutions are country-specific. Globalization and international cooperation are the two causal factors that made the technology into the monster that it is today.

While there is some importance to what they have to say, some of their concerns are becoming more easily mitigated. For example, Morozov's thoughts on governments adapting technology may work in an ideal society but lose credibility when we begin to understand how technology begins to shape society and how the government needs to interact with it. A government's stubborn refusal to adapt to the technology in use can significantly weaken their ability. Arguments relating to the physical layer of digital networking are weakening more with the increasing strength of satellite-based communications. The satellites are placed outside of any government's territory. Satellite-based internet is a growing trend that may lead to even more advancements in the system. By minimizing the amount of the physical network layer that exists in a country, the impact of the country on how technology operates reduces as well.

School Three - Diffusion

This school focuses on the power shift away from larger governments for varying technical reasons. This power shift significantly happens because of the increasing technical capabilities of corporations and other organizations or groups, as scholars note. The increased technical capacity from ideas like Moore's Law, which states that the effective processing power of computers doubles every 18 months, to the lower cost of such processing helps non-state actors attain power that previously only the government could really have. Without such technology, as an example, Anonymous, a semi-anarchic group of hackers who use their technical skills to harm entities that they view as nuisances, would not be able to exist in power or in theory. In addition, these tools have paved new roads for smaller countries to take in the world of espionage, such as the Stuxnet worm which ruined several Iranian reactors (Zetter, 2014). While this worm was designed in part by the U.S., the only reason it could work was because of the developed infrastructure within Iran and around the globe that allowed for its successful transmission. Several scholars have noted, as well, that all governments must consider new digital means of interaction with the world as a result of this growth. Because this school is more focused on what is happening now in comparison to more of a retrospective look presented by the Centralization scholars, Diffusion is the stronger model for the impact of ICT on major state power.

Previously, the only entities that could interaction with states were other states. Former Secretary of State Henry Kissinger argues that individuals now possess the power to significantly interact with state in his recent book (2014). While he acknowledges that the tools are only bad if used to harm the state, he also said that the power that an individual has is extremely high right now. A single person with enough technical capacity can down key infrastructure like power plants both domestically and internationally. The challenge presented is that the actors from a smaller country could target key areas of a larger country, whose own cyber forces would not be able to respond in the typical reciprocal manner that such physical attacks used to be done. This asymmetrical response is only further proof of the diffuse power that is held by non-state actors.

By reorganizing the government's intelligence services, individual state power can be effectively reduced. Jane Harman (2015), a former U.S. congressional representative, describes in her essay how the U.S. government has fallen behind in its intelligence systems. Her vision of the future sees a shift in how the CIA and NSA operate, with the CIA potentially integrating drones as part of an increase of its paramilitary to engage in covert acts, and the NSA shifting to more offensive measures rather than its existing data mining setup which is easily shifted over to private contracting. This sort of shift is clearly plausible, especially the NSA shift, given the amount of data mining corporations currently do. While, on the surface, this may seem to strengthen the government, consider that the only way the NSA would be maintaining their existing surveillance structure would be through integrating the information gathered by private contractors.

In some cases, power is taken away from, instead of given away by, those who have it. With a heavy focus on the Anonymous collective, Professor Taylor Owen (2015) analyzes the effects of groups who intend to disrupt the power of government control. This disruption, he argues, shifts the power away from governments to groups who disrupt. Such groups now have the power that governments used to have exclusive control over. The diffusion of power to groups like Anonymous demonstrates the position the U.S. is in with regards to control. This shift is only possible because of the significant amount of ICT in place.

Part of why the Russians would be able to defeat Napoleon was their scorched earth strategy. By minimizing what the French would be able to obtain from the land, the Russian forces would be able to eventually overpower the French as they continued deeper into Russia. These ideas of diligence and caution help reduce the impact that government surveillance can have on individuals. While Ronald Deibert (2013) and his book focus on the whole of the internet, it does have implications for state power, as he discusses. Part of state power includes the ideas of keeping information secure, according to his arguments, and that we need to be thankful for and careful with what technology has done for society. By being cautious and observant about what is being done with the internet, we can protect it without it becoming more out of control than what has already happened.

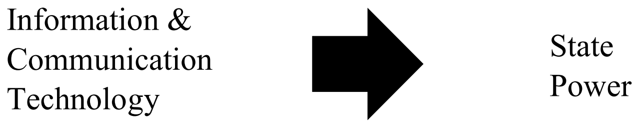
Information is power. Those who have accurate information wield more power than those who do not. So when anyone can access vast amounts of information on the internet, they gain a degree of power. With their general focus on the internet, Eric Schmidt, the current executive chairman of Google, and Jared Cohen, the head of Google's think tank, promote the idea that the U.S. government has lost a degree of its centralized power because of ICT through historical contexts (Schmidt and Cohen, 2013). They argue that new forms of distributing information help shift the power away from the main holders to the common people. Their projections on ICT growth include connecting a vast majority of the world by the end of the first quarter of the century. As part of this technical proliferation, the authors note that people will lose some of their privacy and security. With technology recording seemingly everything, governments and corporations will have a slight edge in this regard, but the authors argue people can keep some of this information secure with vigilance.

Through their analysis of cybersecurity issues and tools, Singer & Friedman (2014) look at a number of cyberattacks such as the "Stuxnet" worm as part of their discussion on the importance of cybersecurity. Their global focus demonstrates how diffuse power has become as a result of technology. As part of their response to the problems presented earlier in the book, these policy makers look specifically at the diffusion of information and other methods of transparency to aid in defense, which shifts the power away from the US government.

The idea that relative state power, much like energy, is a conserved quantity seems to make sense, as governmental power is only shifted between actors, is either taken from or given by the people the state rules over and is neither created from nowhere nor destroyed. While this may be arguable, the impacts of it here do deserve a mention Therefore, more countries gaining some power means either individuals or other countries must lose it. By looking at a history of intelligence, with a particular focus on the intelligence war between the US and the USSR, government historian Michael Warner (2014) investigates the effects of ICT on intelligence gathering. In particular, towards the end of the book, he describes how the entering the intelligence community has become easier for smaller countries to enter. By decreasing the entry cost for countries, it decreases the control that the US has had on intelligence gathering since the Cold War ended and thus their power by dropping the advantage they have over other countries. This lack of control helps to increase oversight on intelligence services.

While their means are different, their observations point to the same basic conclusion: the balance of power has shifted away from the U.S. government. Whether it is from a group like Anonymous who works against some of the U.S. government's interests, from within to optimize services, from new innovations, from ordinary people trying to protect themselves, or from some other source such as a nation's intelligence service, all result in the power being taken from those who are currently holding the most. Without technology, we would not likely see many of these being options. In addition, it is unlikely that we will see some of these factors going away any time soon. Because these different components both have already shown their impact on the government and seem to have fewer negative consequences than those in the Centralization school, Diffusion represents the most insightful picture for how ICT impacts governments.

Model & Hypothesis



The specific hypothesis I will be considering is that a growth in ICT results in a decrease in the power of state actors, but that power can be regained through the intervention of non-state actors utilizing three specific case studies. While there are other examples, I believe these three studies each demonstrate a different aspect of the issue which, when brought together, will support my hypothesis. These three case studies include both state and non-state actors.

The first case is the Office of Personnel Management hack, an attack against a state actor. The second case is the work of the Syrian Electronic Army, a non-state actor that works offensively. The third and final case is the San Bernadino fallout with Apple and the FBI and how state and non-state actors behave in conjunction with each other. Table 1 summarizes this information.

These case studies were drawn from major events happening over the past few years where technology played an integral component. Recency is crucial in this area as technology is constantly evolving and improving. If we look too far back, it becomes too difficult to draw sound conclusions from the case as the technology in play is weaker. Information on these cases was drawn from credible news outlets and reports over the same time frame. Considerations of why each case was chosen rather than its contemporary counterparts will be brought up as each case is addressed.

Table 1: Case Studies and Actors

Case Study	**State Actor Key?**	**Non-State Actor Key?**
Office of Personnel Management	Yes	No
Syrian Electronic Army	No	Yes
Apple & FBI	Yes	Yes

These three case studies demonstrate a clear line of thinking. The first case presents the general weakness of a state actor. The second will show how a non-state actor begins to interact with a state actor independently and what sort of power a non-state actor has. The third case synthesizes these two by looking at how a non-state actor modifies the relative power of a state actor with whom they are cooperating. In looking at the combination of all three cases, we will then draw some conclusions to help us understand how technology interacts with the power of the state.

Case Studies

The first case we will be considering is that of attacks made against the Office of Personnel Management or OPM, the part of the federal government that handles a lot of the human resource affairs for the federal government. Over the past year, the OPM was hacked which resulted in the illegitimate access of personal data of anyone who had any sort of interaction with the federal government which includes such interactions as background checks. While the true perpetrator of the attack is unclear, there are some indications that the attack came from China. While this attack was specifically against the United States, extending the case to include another country would not be difficult. In any case, this attack demonstrates the weakness of the state defensively.

While there are numerous cases of companies being hacked, the OPM hack strikes a balance of being both semi-recent and a state target. Any case that would include a non-state target loses validity as it leaves the scope of this project. In addition, technology develops at such a rapid pace that looking too far back also creates invalid results as either party may have new systems in place. This is just one major example that satisfies both timing and targeting.

Now, regarding the case study on the OPM hack, this case study will demonstrate a weakness of the centralized defense mechanisms especially on the part of states. This attack resulted in the leaking of Personally Identifying Information, or PII, for 4.5 million people (Davis, 2015). Such information typically includes things like names, addresses, health records and historically also includes things like Social Security numbers. This information then may be used in the acts of identity theft.

While this is very detrimental to the people who had their PII compromised, this also has a high degree of fallout relating to the federal government. First, the government struggled to immediately determine the fallout of the breach including who all may have been affected by it. This is a poor reflection on practices relating to internal organization of data (Shieber, 2015). Second, and more significantly, this attack demonstrates a generally weaker security posture on the part of the federal government in comparison to the offensive capabilities of other entities, both public and private.

Once we understand that the defenses of a state are weak, it takes very little to come to the conclusion that the offensive capabilities of the same state are just as weak. When every actor has access to the same basic tools and mechanisms, knowledge relating to the capabilities of those tools starts a feedback loop between the offense and defense. Actors who are competent in both may notice a bug in their defenses that allows for someone to exploit it for nefarious purposes. They then will patch this with a more secure mechanism. After this, they may start to think how to crack it, as other actors may notice the same flaw and patch it as well. This process of defending, trying to break the defenses, fixing the weak points and looking at how to break the newly bolstered defenses creates the strongest possible network. Figure 1 illustrates this sort of thinking.

When an actor fails to find a weakness, one of two things must be true. Either the system is invulnerable and there really were no weaknesses to be found or the actor's process of exploitation was flawed in some way that caused the weakness to go overlooked. In this specific case, the hack proves the system was vulnerable and therefore, the government's process for attacking their own systems was weak.

This idea also implements a logical rule, *modus ponens*, which says that if the outcome of a simple conditional "if…then…" statement is true, then the condition must also be true. In this case, the statement would be, "If an actor has a weak digital offense, then they have a weak digital defense." It is clear that the latter is true in this case study,

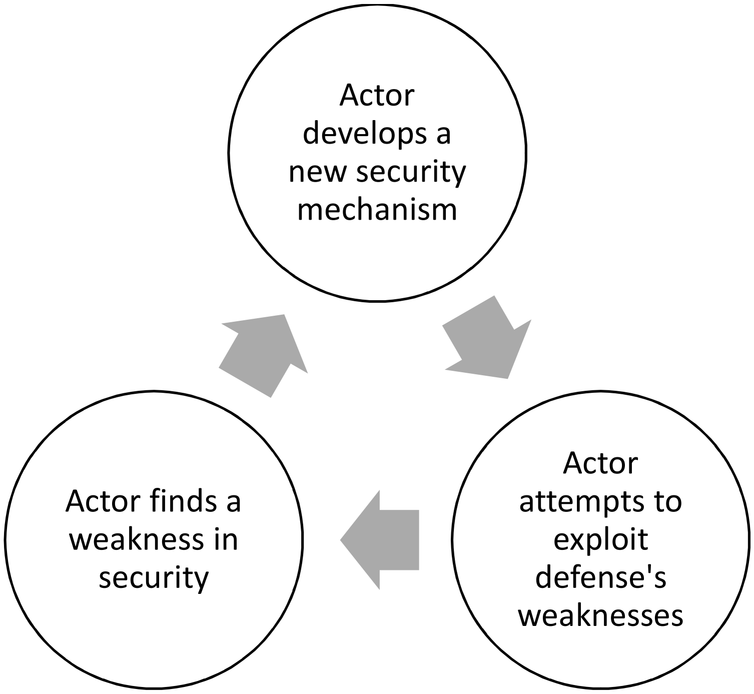

Actor develops a new security mechanism
Actor attempts to exploit defense's weaknesses
Actor finds a weakness in security

Figure 1 – Security Testing Process

which provides us some evidence to suggest that the former should also be true. The only flaw this may have is if we have sufficient reason to believe that the statement itself has some error in its thinking. However, the process of testing defenses seems to indicate this may be true. In summary, the weaknesses of the U.S. government demonstrated by the OPM hack are indicative of systemic weaknesses of state actors. However, non-state actors are completely different consideration.

The second case is that of the Syrian Electronic Army. The SEA is a set of independent hackers who assist the Assad regime and the Syrian Government as they proceed through their civil war. These hackers have been responsible for numerous attacks against digital U.S. targets. Without the aid of these independent hackers, however, these breaches may not have ever happened. The intervention of a non-state actor allowed for the furthering of a state-actor's cause.

While there are other non-state actors, like Anonymous, who are consistently interacting with highly-sensitive entities, the SEA has a unique distinction of being officially independent of the state while still supporting it. Anonymous and their anarchical contemporaries do not make good examples. They are far too unpredictable and work more as vandals raiding the internet and causing problems either with an individual site or releasing information to enable others. While some of the SEA's attacks may appear random, they at least relate back to support of Syria in some regard. Looking at the SEA gives us a stronger, more predictable actor who can provide better general insights.

In light of the Syrian Civil War, which has been going for the past five years, the Assad regime works to actively fight the rebels. However, state powers have already been shown to not have the strongest cyber presence. In light of this fact, numerous hackers came together to form the Syrian Electronic Army not long after the civil war began. This group works on behalf of the Assad regime to cause problems on the internet for the government's opponents, but their exact relationship with the regime is unclear (Perlroth, 2013).

Like many other hacking groups, the SEA works more as vandals causing problems for sites than breaching databases gathering information. However, this sort of work in taking down a site is a more fundamental type of attack. In a process similar to "ARP Spoofing", hackers can convince the core systems of the internet that their own site is the real site and to direct all appropriate web traffic to them by poisoning reference servers and using their own servers as an imposter. While this may not be the exact method they use, it is one process they can use.

The SEA, however, has gone far beyond that in some of their efforts. While the United States has caught in and arrested a few members of group, the efforts of the SEA have gone to trying to gain illegitimate access to some information from the US government and its employees is growing (US Department of Justice, 2016). Their work has included going so far as developing and releasing ransomware, specialized malicious software that locks up a computer until the user pays the developer a pre-determined amount of money to release it, in order to help finance operations. The efforts of the SEA show the power that a non-state actor has over others, including state actors. What is important, though, is to see what happens when both interact.

The third major case we will be considering is the case between Apple and the FBI where the latter attempted to get the former to develop tools to eventually allow them access to the phone taken from the San Bernadino shootings before an independent third party developed the tool. The fact that the FBI was unable to decrypt the data on the phone or develop the system to bypass the auto-erasing mechanisms built into iPhones where the iPhone automatically erases the data on the phone after 10 failed attempts independently is an indication of the initially weak state of the state to crack encrypted data as well as the superior abilities of non-state actors to both develop tools to encrypt and decrypt data.

Apple serves as a stronger case study than another mobile developer for two major reasons: their vertical integration and the resulting strength of their encryption. Because the only devices that can use Apple's software like the iOS mobile operating system are Apple products and because Apple can control the technical specifications on these products, Apple is able to make their software operate in a more narrow way. The Android platform, Apple's main competitor for mobile operating systems, is rooted in an open source system rather than an entirely proprietary Apple product, meaning that a user can easily engineer additional aspects for Android by looking at the code which is public available. This also means that some of the encryption mechanisms have to be made public knowledge. In addition, the Android system is usable on phones from a number of different producers, meaning they have little to no control on the specifications of the phones. Because of this, Android's encryption is only as strong as the weakest device it can be used on, which can be relatively cheap by smartphone standards (Groll, 2016).

While the previously mentioned RSA is most commonly used for secured internet traffic and has a number of other safety features built in such as digital signature which verifies the information had to have come from the person who claimed to have sent the message, the basic mechanics of such a system are common throughout. With regards to mobile technologies, however, encrypting the data on the device through the use of passwords was important in case sensitive data was on the device and it were to be stolen by a malicious entity. However, companies used to maintain mechanisms for what was called a “backdoor” into the device where the manufacturer developed the encryption mechanism in such a way as to give them a means to access and decrypt the information on any device running the operating system whether or not it had a password. With modern versions of the mobile operating systems, though, companies have foregone their ability to do so as a result of public backlash. For example, Apple gave up their backdoor with the implementation of iOS 8 back in 2014, and Google listed their plans to match this in the next Android OS update (Green, 2014).

The lack of this universal access mechanism is part of the current issue between the federal government and Apple. In the past, federal entities have requested that Apple break the encryption on a device to allow proper authorities to access it using the All Writs Act of 1789 which requires any entity to provide support to an investigation when asked by a federal judge, which Apple has done without question in the past when using previous versions of its mobile device operating system iOS. Apple refused to comply in this case because they presently lack a means to access the information on the device. Their previous compliance with the All Writs Act was rooted in their having a universal access mechanism on iOS versions prior to 8. Because of their refusal, the FBI is attempted to force Apple to develop a tool that, instead of creating another backdoor access into the encryption, would get rid of the threat that comes with simply trying to guess the passwords through what is known as “brute force” hacking, where a hacker merely enters many passwords in the hopes that one will unlock the service. Current security mechanisms built into the operating system the phone is running will delete all content on the phone after 10 failed password attempts, which the FBI is wanting removed (Apple Inc., 2016).

By looking at how the FBI interacted with Apple, something is made clearer: the FBI previously couldn't technically break the encryption on the device while independent hackers claimed to be able to. If they had the technology in place to either create backdoor access or to remove the security features of the OS, they would be doing so without having to work with Apple. The strength of the encryption mechanisms built into the iOS operating system and its underlying source code can indicate that the government has fallen behind in their efforts to attack an encrypted system successfully. As an extension of this, some have speculated that countries such as China and Russia would demand access to the same tool as a means to further spy on their citizens to deepen their control of their respective countries.

While some may try to argue that this encryption system is also working against Apple and may be generalized to include other corporations who use similar systems, it is important to note that Apple is refusing to develop the tool for bypassing the passcode, not that they are unable to do so. Apple knows heuristically what it would take to develop the mechanism to break the encryption insofar as it removes the safeguards built into bad password attempts. They have constructed the DIST they use, so they know they can't break the actual encryption itself but that they can break the other protocols they have written in.

However, this case took an unexpected turn. In late March, the FBI dropped their case against Apple when an independent hacker stepped forward to develop a tool for them to use. While the case has come to a conclusion with the FBI having their mechanism, some may try to argue that this has shown the power the state has over the individual. However, there are two notable critiques of that argument. First, the FBI did not come up with this tool internally. The system they used was developed by an unnamed non-state actor. This demonstrates further the restoring effect that non-state actors have when cooperating with a state power. Second, this tool is very narrow in its capabilities. The director of the FBI claims that this tool will only work on the type of iPhone that they required access to, the iPhone 5c, and no other newer devices. As this device has been discontinued, the lasting impact of this tool is low (Medhora and Volz, 2016).

In the end, this case demonstrates several things. First, the state of DIST does not favor the government. We are in a place where the modern system to keep data secure has no means to bypass the protection as the cracking tool only works on a single model of device which is no longer being made. Second, the government was unable to come up with the tool on its own and had to rely on an outside actor to develop it. Third, non-state actors are the true power players in interacting with ICT. Through these three observations, we can draw a few conclusions.

Conclusion

Looking at each of these three case studies individual and together demonstrates a few things. First, the two case studies with key state actors – the OPM and Apple cases – demonstrate the general weakness of state actors on the electronic front. Second, the two cases with key non-state actors – the SEA and Apple cases – demonstrate their general strength on the electronic front. When we look at how the Apple case combines both state and non-state, we see that it is only through the intervention of a non-state actor that the state is able to assume a level position with non-state actors. Thus, it is clear that non-state actors play an integral role.

This supports the proponents of the Diffusion school. Evidence supporting the Centralization school would see the reverse of what happens here, with the state able to do what non-state actors cannot. For the Skeptics, the capabilities of each side would appear to be even and minimal. However, the threat that the Department of Justice sees in the members of the SEA, going so far as to put them on the Most Wanted list for Cyber says otherwise.

Looking forward, though, this balance may change. What the government lacks in capabilities, it can make up for in funding research and development that non-state actors may struggle to match. By coming up with new mechanisms to bypass defenses and protect themselves, state actors may be able to gain leverage. However, any leverage is lost when the social aspect of defenses is breached when people leak the government's processes and tricks.

Technology is here to stay; that fact is a guarantee. Beyond that, the number of different types of systems which interact with the internet is growing rapidly as well, including toasters that print the weather forecast for the day on toast. One notable trend in this analysis of the so-called "internet of things" is the implementation of "smart home" technologies. These are items such as lightbulbs, thermostats, security cameras and more that are connected to the internet through a central controlling unit in the house.

The premise is that someone with internet access can log into their home and turn on the thermostat or lights before they get home to make their house more ready for their arrival in advance. While this system seems futuristic and interesting, it also poses a danger in that without a strongly secured connection between the controller and the internet, a hacker could break into these devices and theoretically cause damage to the house. While this has fewer implications in the greater context of this paper immediately, this same technology can be used in larger corporations and offices to help save funds by allowing more remote control of services. A breach in these sorts of systems might grant a hacker access to the whole network if the breach is significant enough. Plus, offices may implement additional devices with internet connectivity that can also be hacked with major consequences.

The Internet, as it stands now, is a powerful force with great potential to be used for both good and evil. Those who will use it for good know how it will benefit society and will continue to look for ways to make it better. Those who use it for evil will find ways to keep breaking through the protections and hack into systems to cause problems. If we reach an era where the Internet is supplanted by a superior technology, society will at least be able to look back and see what a significant impact it had for its existence.

References

Apple Inc. (2016, 16 February). *Answers to your questions about Apple and security.* Retrieved from http://www.apple.com/customer-letter/answers/

Crouch, A. (2008). Culture Making: *Recovering our creative calling.* Downers Grove, IL: InterVarsity Press.

Davis, J. H. (2015, 9 July). Hacking of government computers exposed 21.5 million people. *New York Times*. Retrieved from (http://www.nytimes.com/2015/07/10/us/office-of-personnel-management-hackers-got-data-of-millions.html?_r=0)

Deibert, R. J. (2013). *Black code: Surveillance, privacy, and the dark side of the internet*. Toronto, Ontario. McClelland & Stewart.

Dover, R. (2014, 3 July). The world's second oldest profession: The transatlantic spying scandal and its aftermath. *The International Spectator: Italian Journal of International Affairs.* 49:2. 117-133. doi:10.1080/03932729.2014.904989

Green, M. (2014, 23 September). Is Apple picking a fight with the U.S. government? Not exactly. *Slate*. Retrieved from http://www.slate.com/articles/technology/future_tense/2014/09/ios_8_encryption_why_apple_won_t_unlock_your_iphone_for_the_police.single.html

Greenwald, G. (2014). No place to hide: *Edward Snowden, the NSA, and the U.S. surveillance state*. New York, NY: Metropolitan Books.

Groll, E. (2016, 18 February). Why Apple — and Not Google — Is in the FBI's Crosshairs: Google can't encrypt its phone data as well as Apple. That's bad news for its customers -- and good news for the government. *Foreign Affairs.*

Retrieved from http://foreignpolicy.com/2016/02/18/why-apple-and-not-google-is-in-the-fbis-crosshairs/

Harmon, J. (2014). Disrupting the intelligence community: America's spy agencies need an upgrade. *Foreign Affairs, 94 (2)*. Retrieved from http://www.foreignaffairs.com/articles/143042/jane-harman/disrupting-the-intelligence-community?cid=nlc-foreign_affairs_this_week-031915 - disrupting_the_intelligence_co_5-031915&sp_mid=48266214&sp_rid=c3dhYWxrZXNAbWFsb25lLmVkdQS2

Kissinger, H. (2014). *World order.* New York, NY. Penguin Press.

Medhora, N. and Volz, D. (2016, 7 April). FBI director says unlocking method won't work on newer iPhones. *New York Times.* Retrieved from http://www.nytimes.com/reuters/2016/04/07/technology/07reuters-apple-encryption-fbi.html?_r=0

Morozov, E. (2011). *The net delusion: The dark side of internet freedom.* New York, NY. Public Affairs.

O'Harrow Jr., R. (2006). *No Place to Hide*. New York, NY. Free Press.

Owen, T. (2015). *Disruptive power: The crisis of the state in the digital age.* New York, NY. Oxford University Press.

Perlroth, R. (2013, 17 May). Hunting for Syrian Hackers' Chain of Command. *New York Times.* Retrieved from http://www.nytimes.com/2013/05/18/technology/financial-times-site-is-hacked.html

Schmidt, E. & Cohen, J. (2014). *The new digital age: Transforming nations, businesses, and our lives.* New York City, NY. Vintage Books.

Shieber, J. (2015, 17 June). US Government Begins Outreach To Office Of Personnel Management Hack Victims. *TechCrunch.* Retrieved from http://techcrunch.com/2015/06/17/us-government-begins-outreach-to-office-of-personnel-management-hack-victims/

Singer, P.W., & Friedman, A. (2014). *Cybersecurity and cyberwar: What everyone needs to know.* New York, NY. Oxford University Press

Tucker, D. (2014). *The end of intelligence: Espionage and state power in the information age*. Stanford, CA: Stanford University Press.

US Department of Justice (2016, 22 March). *Computer hacking conspiracy charges unsealed against members of Syrian Electronic Army: Two fugitives believed to be in Syria added to FBI cyber's most wanted* (DoJ publication No. 16-329). Washington DC: U.S. Government Printing Office.

Van Creveld, M. (1996). The fate of the state. *Parameters*, *Spring 1996.*

Villasenor, J. (2011). *Recording everything: Digital storage as an enabler of authoritarian governments*. Retrieved from http://www.brookings.edu/~/media/research/files/papers/2011/12/14-digital-storage-villasenor/1214_digital_storage_villasenor.pdf

Warner, M. (2014). *The rise and fall of intelligence: An international security history*. Washington, DC. Georgetown University Press.

Wolf, M. (2001). Will the nation-state survive globalization. *Foreign Affairs*. Retrieved from http://www.foreignaffairs.com/ariticles/56665/martin-wolf/will-the-nation-state-survive-globalization

Zetter, K. (2014). *Countdown to zero day: Stuxnet and the launch of the world's first digital weapon*. New York, NY. Crown Publishers.