The Economics of Cybersecurity and Cyberwarfare: A Case Study

Lorenzo Carrazana

December 5, 2018

ECON Colloquium

Dr. Herbener

1. Introduction

Throughout the millennia of human conflict, warfare and security have experienced several revolutions in their domains. Warfare once based only on land evolved to include the sea. Eventually, states were forced to also consider the use of airpower in providing security, adding a new dimension. However, within the past couple decades, states are now recognizing cyberspace as a new domain of warfare and a place where they must consider the challenges it poses to the provision of national security. Cybersecurity especially in the context of cyber warfare offers defense policy challenges that hold similarities, yet fundamentally differ from those of conventional warfare. Under the US Constitution the Federal Government is given the power to provide national defense. Ultimately, however, the aggregated cyber security actions undertaken by individuals and firms represent the bulk of the national cyberwarfare defense. Furthermore, in the United States the primary provision of national cybersecurity defense is best suited to private entities, however; the lack of a clear federal cybersecurity policy creates a degree of policy uncertainty that contributes to a less secure cyber realm. Finally, private entities must overcome the unique challenge cyberattacks pose, as they are capable of seriously hampering the price system by reducing access to relevant prices and capable of significantly disrupting the scope of the division of labor. This paper will examine the case study of the notPetya cyberattack in the context of economic theory and address how policy can be oriented towards promoting the most effective provision of cybersecurity.

Why examine the economics of cybersecurity? Since the emergence of the nation-state, national security is a good that has traditionally been provided by the state. States have developed the means to adequately defend their geographical area of control against conventional weapons and forces, however, they do not have the same capability to defend their

territory against cyber threats. An understanding of the economic challenges cybersecurity poses to policymakers in crafting a strategy to provide national defense is crucial. The provision of cybersecurity, whether or not at a national level, comes with associated costs and benefits along with varying incentives based on the institutional "rules of the game". Furthermore, cyberwarfare is a modern iteration of total war that, that among other things, targets a nation's economy (Smeets 2018). Specifically, cyberwarfare can target a nations capacity to engage in production for warfare and production for general consumption, rather than only targeting the military forces of a nation. Lastly, cyberattacks are not an uncommon threat to firms. Surveys show that ninety-seven percent of fortune 500 companies admit that they have been hacked (Stanton 2018). Therefore, a state tasked with providing national defense must be concerned with the economic effects of cyberwarfare.

The National Research Council defines a cyberattack as, "deliberate actions to alter, disrupt, deceive, degrade, or destroy computer systems or networks, or the information and/or programs resident in or transiting these systems or networks" (Singer, 2013). Cybersecurity and cyberwarfare are complex topics where the discussion can easily become highly technical and theoretical, approaching subjects requiring specialized knowledge in computer science. Using a case study helps make understanding cybersecurity more straightforward and provides context for the theoretical concepts. The Cyberattack colloquially called "notPetya" on Ukraine in June 2017 provides useful insights and a solid foundation as a case study for the subject of the economics of cybersecurity and the costs and benefits of related policy options.

2. Examining notPetya

On June 27th, 2017 malware as part of a broader scale Russian cyberattack on Ukrainian infrastructure infected the network of a Maersk office in Ukraine. Within seconds of infecting a

computer, the malware would permanently encrypt the hard drive, effectively erasing all the information stored on the machine. The virus, called "notPetya" due to its technical resemblance to an earlier Russian ransomware virus named "Petya", rapidly spread across Ukraine and throughout the world (Fruhlinger, 2017). Once inside Maersk's network, for example, it was able to spread to other Maersk offices, servers, and port facilities with relative impunity. "To date, it was simply the fastest-propagating piece of malware we've ever seen," says Craig Williams, director of outreach at Cisco's Talos division (Greenberg 2018).

Ukraine, however, was devastated by the virus. In a matter of hours, an estimated 10% of all computers in the country were destroyed. The attack affected several hospitals, banks, airports, and credit card payment systems all throughout the nation. While the cyberattack was 'aimed' at Ukraine, it caused tangible effects worldwide, speaking to the complex nature of the downstream effects of cyberattacks. Estimates place the total cost of replacing equipment lost in the cyberattack at about $10 billion, including at least $300 million to Maersk alone, making it the costliest cyberattack to date (Greenberg 2018). However, the details of the attack on Maersk serve as a helpful case study on the economic effects of a cyberattack and inform policy makers on how to address the subject of cybersecurity.

A large amount of the data destroyed on Maersk computers were not simply being stored for future use but were actively being referenced for day to day business operations. The attack disabled the entire computer network for the company, affecting seventy-six port facilities and 800 seafaring vessels, representing $1/5^{th}$ of the worlds shipping capacity (Olenick 2018). Although the majority of the Maersk cargo ships at sea were unaffected, the situation at the ports was dire once the global network running shipping logistics went offline. Terminal operators at ports not only had no way to know what was to be unloaded from the container ships as they

were coming in to port, and no way to know which containers were to be loaded onto which ships, but also no way to tell where unloaded containers were to be sent from the port terminal. The resultant backlog created a multi-mile long jam of truckers waiting to enter or leave port terminals and forced container ships to idle offshore, unable to dock (Greenberg 2018).

Furthermore, the virus knocked out nearly all the 150 domain controller backup servers Maersk had spread across the world. Although after several days Maersk was able to find backups for most of their individual servers and computers, they could not integrate their network without a functioning domain controller. Fortunately, Maersk discovered a lone domain controller in a small town in Ghana that had avoided the virus after its server was taken offline by an unrelated power outage (Greenberg 2018). Although the fluke allowed Maersk to largely restore their network after a few days, normal operations at their port terminals did not return for a week. The firm took no new orders to ship goods for several days and in the confusion, some containers remained lost for months afterwards. By Maersk's own estimates about twenty percent of the products they were transporting stopped moving during the attack (Olenick 2018). Since the company also handles about twenty percent of all international trade, the notPetya attack essentially halted five percent of international trade.

3. Definitions and Theory

If cyberwarfare is a new domain of warfare, it becomes critical to discuss the similarities and differences between conventional and cyberwarfare and attempt to define cyberwarfare and cyberattacks. All war, including cyberwarfare, stands in contrast with peaceful voluntary exchange. Fundamentally, warfare disrupts the free exchange of goods and services, disrupts the division of labor, and directs labor towards destruction, not production (Mises 1949, 817). Conventional war contrasts with voluntary exchange primarily by the substitution of peaceful

transactions for physical violence. A cyberattack, however, may or may not cause physical destruction. Nonetheless, a cyberattack that does not cause physical destruction may be used as part of broader conventional war between states.

Furthermore, cyberwarfare differs from conventional warfare at the operational and tactical levels of warfare. Policy makers and military leaders direct the deployment of conventional forces according to strategic objectives to a certain theater of war (CADRE 1997, 2). Resources for conducting cyberattacks, however, do not need to be deployed to this theater of war, as they can be conducted from anywhere in the world. Also, at the tactical level, rather than troops physically meeting on the battlefield, attacks can be launched by a single person from anywhere on Earth and directed towards a particular battlefield. Although, as seen in the notPetya attack, a cyberattack directed towards a specific region of conflict (i.e. Ukraine) can have far broader direct, and even unintentional, implications beyond the targetted battlefield. This characteristic of cyberwarfare blurs the line between its tactical and operational use.

Nonetheless, the idea of cyberwarfare fits well within the broader phenomenon of total warfare. The concept of total warfare emerged in the late 19th and early 20th century where warfare moved from being primarily between the armies of two or more nations, to encompassing every aspect of nations (Mises 1949, 819). Economies are fully mobilized towards the end of victory over the enemy and are likewise the targets of attacks. With total war, policy makers and military leaders may not see the enemy military forces as the only center of gravity, but rather the economic capability, including the civilian labor force, as a center of gravity to be attacked in order to achieve victory. Cyberwarfare is fully integrated in the concept of total war by its unique capability to not only target military forces, but also the economic capacity of a nation. The notPetya cyberattack was aimed towards the Ukrainian economy and infrastructure

impacting medical facilities, fuel services, banking services, and both private and governmental logistics capability. Globalization, however, has extended the division of labor beyond the borders of any nation. Therefore, a Russian cyberattack intending to damage Ukraine's economic capacity must have international effects. Multinational firms, such as Maersk, operating in the Ukraine suffer harm throughout their worldwide network.

The complex and sometimes unintentional, yet often tangible effects of a cyberattack creates confusion in differentiating between what is a cybercrime, cyberattack, cyberwarfare, or simply a nuisance. For example, is a state engaging in cyberattacks for the purpose of corporate espionage, as China does to US firms a nuisance, a prosecutable cybercrime, or an act of war? Furthermore, how should policy makers, military leaders, and business leaders react to attacks like notPetya? These complications make cyberwarfare more difficult to define compared to conventional warfare. The difficulty in defining cyberwarfare and cyberattacks poses a challenge for policy makers. Especially in the United States where the Federal Government is tasked with the duty of providing national security, policy makers need an understanding of these definitions, insofar as they exist, to determine the proper policy response. Not all cybersecurity breaches necessitate government to remedy a national security concern, however, clear definitions make this decision making less complicated for policy makers.

Published by Cambridge University Press in 2017, the Tallinn Manual 2.0 attempted to clarify the blurry definitions surrounding cybersecurity. The Tallinn Manual is a product of a three-year exercise by an international group of academics at NATO's Cooperative Cyber Defense Center of Excellence in Tallinn Estonia. The scholars included experts in law of armed conflict, space law, human rights, and international telecommunications law (Jensen 2017, 4). The manual provides the most in depth examination of international law regarding what is and

isn't cyberwarfare or a cyberattack, and what is instead a cybercrime or simply a nuisance. This manual is useful for not only helping define complex subjects, but also showing where there exists a lack of consensus among experts in the field. Although the manual provides useful insights in creating standardized definitions, it creates many questions that remain unanswered. For example, the Tallinn manual attempts to address the issue of determining at what point a cyber-operation is a use of force. Rule eleven states that a cyberoperation is a use of force when its result is akin to a direct kinetic attack (Jensen 2017; Stanton 2018). Furthermore, the manual goes on to delineate between a cyberattack and an act of cyberwar, also called a cyber-armed attack. A cyberattack is armed if the attack does physical damage to persons or property, and therefore can be construed as a violation of a state's sovereignty (Jensen 2017). Also, a state sponsored cyber operation targeting sensitive information is not considered a cyber armed attack and does not violate state sovereignty in the same manner as an armed (cyber or otherwise) attack would. Jensen argues, "states have not found espionage to be a per se violation of sovereignty, even when those actions take place in and/or have effects in another state. States routinely outlaw the methods of espionage as a matter of domestic law, but not as a violation of sovereignty" (2017, 8).

Although the scholars generally agreed on this broad definition of a cyber armed attack, they could not find a clear consensus on precisely where to draw the line between physical damage to persons and property, and hence a cyber armed attack, and lesser forms of cyber operations. For example, would locking somebody out of their bank account cause physical damage if they cannot buy food, or heat their house during the winter? If so, is this now a cyber armed attack that can potentially be considered an act of war? The writers of the Tallinn Manual say no, as a brief or periodic disruption of non-essential services is not a cyber armed attack (2017).

Although this guidance answers the question of whether disruption of non-essential that causes some physical harm is *always* tantamount to a cyber-armed attack, it creates new questions that complicate the process of establishing clear definitions.

The Tallinn manual does not explain what determines a brief or periodic interruption of services, as opposed to a lengthy or prolonged disruption. Here the existing literature is silent on determining exactly what constitutes an act of cyberwar. In addition, the manual discusses appropriate countermeasures by states that have been the target of a cyberattack. Rule nine says that states can respond to cyberattacks with "proportional" countermeasures. These countermeasures may be cyber or include other means including diplomatic sanctions or military force (Jensen 2017; Stanton 2018). Although the Tallinn Manual is helpful in establishing a foundation for recognizable definitions, it creates nearly as many questions as it answers. The notPetya cyberattack serves as a clear example of how the guidelines in the Tallinn Manual remove some of the uncertainty, but ultimately leaves questions unanswered.

The Russian cyberattack aimed at Ukraine occurred in the context of a broader proxy war in Crimea. Therefore, the cyberattack was an action undertaken by the Russian government as a means to their end of weakening the Ukrainian government's capacity to govern and establishing de facto control over Crimea. However, what can the Tallinn Manual say about the nature of the notPetya attack? According to the guidelines established by the manual, the not Petya attack was a cyber armed attack, because it caused physical damage by destroying tens of thousands of computers, impacted essential services including hospitals, financial institutions, and transportation services, and affected non-essential services for a significant period of time. Furthermore, by seriously disrupting Maersk and impacting international trade, the cyberattack had incalculable downstream effects throughout the production structure. Companies and

individuals waiting for goods stuck or lost in port facilities incurred costs for their time without the assets they purchased. Of course, not all of these downstream effects could be classified as a long-term disruption of services, but rather brief or periodic disruptions. Also, many of the downstream affects are unlikely to be significant physical effects relative to the physical effects of the hardware directly destroyed by the virus. In addition, the effected multinational companies and the downstream effects have negative consequences in any nation they exist in. With the interconnected nature of globalization, it is likely that some negative effects of the notPetya attack manifested in most nations on earth. The complex consequences also create issues for policy makers in launching countermeasures in response to the attack. Each individual state affected by the attack experienced negative economic effects less than the sum of negative economic effects experienced. Policy makers desiring to respond must determine the level of proportionality of the response of their countermeasures. A state's policy makers must also decide if a proportional response should be based on the extent of the entire cyberattack, the extent of the impact on their nation, some place in between, or no response. In total, the lack of clear definitions and unclear methods to determine proportionality of countermeasures leads to a lack of clear government policy regarding cybersecurity.

This lack of clear policy creates not only increased uncertainty, but a moral hazard where marginal firms tend to rely on the government to provide some degree of cybersecurity protection, leading to a less than optimal provision of cybersecurity in the market. This moral hazard may come about from two ways: 1) The reasonable belief that cybersecurity is a critical part of national security and hence part of the government's mandate in the provision of national security. 2) The threat of government countermeasures will act as a deterrent for cyberattacks. Governments, however, are ill equipped to provide the level of security in the cyber realm

relative to the national security they provide in a conventional context. Even ignoring Fourth Amendment concerns, the US government does not have the resources, manpower, expertise, nor economic calculation capacity to secure every computer in the nation. Andre Kudelski, CEO of the Swiss Cybersecurity firm, The Kudelski group, argues, "One of the biggest challenges we have is that you cannot just make a set of rules and have no more [cybersecurity] issues." (World Economic Forum 2018). Unfortunately, poor, confusing, and outdated policy also contributes to the uncertainty in the market and leads to a sub-optimal outcome of private cybersecurity provision.

The 1986 Computer Fraud and Abuse Act (CFAA) serves as an example of poor policy creating unnecessary confusion, leading to a sub-optimal market outcome. Drafted in 1986, when the computer technology was entirely different than today, the CFAA uses confusing wording and a grossly outdated understanding of cybersecurity to limit private cybersecurity research. The law, "creates unnecessary fear that simple and useful information security research methods could be maliciously prosecuted" (Wheeler 2018, 8). The reduced information security research Wheeler argues, has led to a relative reduction in trained cybersecurity experts and a weaker overall state of cybersecurity (2018, 8). Rather than allow actors to use certain non-malicious scanning tools to detect vulnerabilities within networks, the CFAA disincentivizes such research. Although impossible to know with certainty, in the context of the notPetya cyberattack, vulnerabilities within the tens of thousands of affected computers may have been minimized had the market been able to provide a more optimal level of cyber security, potentially reducing the impact of notPetya.

Although government policy can create distortions in the private provision of cybersecurity, what can economic theory say about potential issues associated with the private provision of

cybersecurity that policy makers should be aware of? First, externalities play a role in the economics of Cybersecurity. Externalities are defined as net costs or benefits an activity imposes on those outside the activity (Coyne and Leeson 2004, 10). Externalities can be positive or negative, with net costs or net benefits respectively affecting that outside of an activity. Conventional economic theory holds that negative externalities will be oversupplied on the market, while positive externalities will be undersupplied by the market (2014, 10). In the context of cybersecurity, the existence of externalities implies spillover effects where the actions of one user can impact other connected users.

The value of each internet connection increases as the total number of internet connections increases. More connections mean more communication, commerce, and entertainment, a positive externality not necessarily internalized by individuals who benefit. When a user fails to secure their equipment, they create a negative externality where other users connected to the first user are marginally more vulnerable to a breach. Conversely, when individuals secure their hardware, they also marginally increase the value of each connection others have with them. Coyne and Leeson argue, “Given this, economic theory predicts that individual decision calculus will yield too little security. The individual undertaking of the security precautions does not internalize all the benefits and will seek to free-ride off the efforts taken by others” (2004, 12). Likewise, those failing to secure their equipment do not bear all the costs associated with their actions. “Therefore, theory predicts that security will be undersupplied by the market and vulnerability, or a lack of security, will be oversupplied by the market” (2004, 12). A common policy approach to address market externalities is regulation. Policy makers looking to regulate the private cybersecurity market to minimize externalities, however, should be cognizant of market responses to externalities

Markets tend to respond to externalities along a few avenues. First, some individuals are motivated by good will, patriotism, and morality to donate to organizations that promote cybersecurity and to apply social pressure to those who fail to secure their equipment. This market response likely does not internalize all the externalities associated with cybersecurity but plays some role nonetheless (Coyne and Leeson 2004, 15). Secondly, bounty programs where firms offer cash rewards for information leading to arrest of hackers are another method to allow for the internalization of externalities. This method, however, is more effective in addressing domestic cyberattacks relative to addressing attacks originating from other states. Thirdly, firms commonly use product tie-ins to minimize negative externalities. Firms regularly offer services bundled with security software. Financial institutions, for example, invest heavily in cybersecurity and bundle it within the services they offer. Firms recognize that consumers demand a level of security in their online activities and therefore respond accordingly(2004, 15).

In addition, the NotPetya cyberattack demonstrated the role externalities play. The malware spread through inadequately secured networks and jumped to other connected networks. Given that notPetya was a malicious attack, it was designed to exploit networks via poorly secured connections, magnifying the negative externalities.

4. Costs and Benefits of Government Provision of Cybersecurity

Given the challenges governments and the market face in providing cybersecurity, what are the costs and benefits of different policy options to address cybersecurity? Governments have three general options regarding the provision of cybersecurity. Admittedly, some of the following policy options are more realistic than others, however, a review of the associated costs and benefits of all three is necessary for an adequate discussion on the subject.

First, governments can take responsibility for the provision of cybersecurity, largely supplanting the private provision of cybersecurity. At minimum this option would require the government to manage the cybersecurity of critical infrastructure. As the state does for conventional national defense, government would take the lead role in providing cybersecurity for private industry, or at least providing it for critical infrastructure as deemed by the Department of Homeland Security (2018). While theoretically the level of cybersecurity could be higher across the board, making the nation not only overall more secure from cyberthreats, but also more resilient in cyberwarfare, one must ask at what cost. Governments have limited resources to engage in the provision of national security. If the Federal Government decided to view cybersecurity as a public good and manage its provision, it would have to secure funding for the national cybersecurity system. According to a study conducted by Business Insider Intelligence, the cybersecurity market will be approximately $655 billion between 2015 and 2020 (BII 2016, 2). If the government intends to provide more cybersecurity than what would be otherwise provided on the market, the cost would likely be greater than this figure. Although a rough estimate, the government should expect to spend at minimum this amount to provide for the national cybersecurity.

Some scholars, however, have noted that the optimal level of cybersecurity is not an elimination of successful cyberattacks, but rather the efficient level of cyberattacks. In effect, the efficient level of cyberattacks is not zero, but rather the amount where the marginal cost of securing against a cyberattack is equal to the marginal benefit of preventing that cyberattack. For example, if the cost to secure against a cyberattack is greater than the cost of the cyberattack itself, the most efficient outcome is the cyberattack. Coyne and Leeson argue, “If the damage done by a breach is greater than the cost of the cheapest means of preventing it, than the breach

is inefficient and should be eliminated. Likewise, if the cost of the cheapest means of preventing the breach is greater than the benefit gained, the breach is efficient" (2005, 8). Policymakers assessing the overall level of cybersecurity in a nation should consider this optimal level of security when deciding on policy.

Although it is difficult to estimate the potential costs of a cyberattack, private companies using the profit and loss system are best suited to finding the optimal level of cybersecurity. Without the profit and loss system, governments are more libel to produce a less optimal level of cybersecurity relative to the market (Mises, 1922). Firms must deal with three primary costs of cyberattacks as part of their calculus to determine the efficient level of cybersecurity (Singer 2014). First, firms must assess the cost of being offline. Each hour offline has costs to firms. Maersk, for example, was unable to utilize its network to coordinate shipping, nor accept new orders for days after the attack. Fundamentally, firms will value time lost online differently according to time preference. Therefore, each firm is best suited to determine the associated costs of being offline relative to the costs of maintaining some level of cybersecurity. The government, however, does not have the capacity nor incentive structure to engage in the same calculus.

Secondly, firms must deal with the cost of paying specialists to repair damages. This cost can vary widely depending on the nature attack and the magnitude of the damage. In the notPetya attack, Maersk had to pay tens of millions of dollars and hire technicians to replace destroyed hardware. A government with the mandate of providing national security defense would necessarily be tasked with replacing and rebuilding damaged or destroyed cyber security infrastructure within firms. Overall, this policy option would require a significant amount of central planning over large swathes of the technology sector of the economy to provide a

national cybersecurity defense comparable to the current provision of conventional national defense. As a result, extreme inefficiencies would emerge from the reduction in market forces.

Thirdly, firms face the cost of losing reputation among consumers (Singer 2014). Firms often rely heavily on their reputation to maintain market share. When consumers do not view a company as reputable it will lose revenue, all else held equal. Interestingly, when polled less than one-third of firms reported factoring in a reduction in reputation after a cyberattack. However, more than seventy percent of consumers polled said they hold a lower view of a firm after it has been hacked (Stanton 2018). Some firms, like Maersk, recognize the importance of cybersecurity, not only to protect their assets and information, but to gain an advantage over competitors. The Maersk chairman stated, "We found we were only average when it comes to cybersecurity. Now we want to become a company where our cybersecurity becomes a competitive advantage" (Olenick, 2018). He also noted the remarkable speed of the company in fully restoring its network within ten days when initial estimates had the restoration process taking up to six months. Firms, therefore, have the incentive to increase their level of cybersecurity based on protecting their reputation. A government, however, tasked with the provision of national cybersecurity, does not have this same incentive.

Policymakers also have the option to play some role in the provision of cybersecurity. Admittedly, this policy option is broad category of policy options that includes any mixture of both government provision of cybersecurity and private provision. Nonetheless, this option will most likely be the outcome given the current political climate. With countless possibilities for various levels of public and private provision of cybersecurity, this discussion will focus on two examples that are current US policy.

Currently, the US government operates as a training pipeline for cybersecurity experts (Singer, 2014). Individuals work for the government agencies including the NSA, DoD, and CIA, where they acquire cybersecurity skills engaging in both offensive and defense cybersecurity. Given that the Federal government (along with the Russian and Chinese governments) have the most advanced cybersecurity operations in existence, those coming out of this pipeline into the private sector are be very well trained. Furthermore, the former government employees often have direct experience in engaging in both offensive and defensive cybersecurity operations. This experience puts government trained cybersecurity experts at a relative advantage compared to their privately trained counterparts because private cybersecurity firms cannot legally engage in offensive cybersecurity operations like governments can. The experience in both offensive and defensive operations creates more knowledgeable experts who are more capable of providing superior cybersecurity services in the private sector. However, this benefit comes with the cost of potentially having a crowding out effect on the private labor force for cybersecurity. Currently, the US government spends roughly $100 billion annually on cybersecurity related operations and agencies, enough to significantly influence the cyber security market (Singer 2018). Lastly, policy makers should remain cognizant of the aforementioned concept of the efficient level of cyberbreaches and the related economic calculation issues.

Secondly, the United States cybersecurity agencies maintain a lose partnership with major industries that tend to be targets of cyberattacks. The government alerts companies of potential threats and assists to some degree in preparation. For example, the NSA has worked with Google and several firms in the finance industry by warning them of potential impending threats. A benefit of this policy is the government's ability to use coercive means to acquire information

and gather intelligence on potential threats that is not available to private firms. US intelligence agencies have the means to acquire information largely unavailable to private firms. However, this does pose the risk of creating a moral hazard and perverse incentive where firms invest relatively less in cybersecurity and instead rely on the government to direct them on the nature of potential threats.

Current US cybersecurity policy fits within this second broad policy option of playing some role in the provision of cybersecurity. This option relies on less government intervention onto the private provision of cybersecurity, yet policy makers must remain aware of distorting effects intervention may have in the total supply of private cybersecurity.

Thirdly, the US government has the option to play no role in the cybersecurity of private firms and to only focus on the cybersecurity of government assets. Under this policy, government agencies would have to take concerted efforts to only manage threats to their own property and not release any information to private firms regarding cybersecurity. Unlike current policy, intelligence agencies would not share any gathered information on potential cyber threats. In addition, to reduce the crowding out effects on labor, government agencies would have to significantly reduce their employment of cybersecurity analysts. Although this policy would allow the least encumbered operation of the market, the reduction of the government capacity to use cybersecurity as a component of its broader mandate to provide security may have serious national security implications and create vulnerabilities among both government and private assets. The United States is unlikely to adopt a policy that minimizes the role the state plays in the provision of cybersecurity, however, policy makers must be aware of the necessary balance between allowing a private market for cybersecurity to operate, and to fulfill its constitutional mandate to provide national defense.

5. Market Resiliency to Cyberattacks

The nature of cyberattacks and cyberwarfare poses a unique risk to the market system by being especially adept at disrupting the price system and quickly reducing the scope of the division of labor. For a nation to win a war, it must reduce their enemy's capacity to wage war effectively. While conventional attacks can physically destroy infrastructure and assets, cyberwarfare can eliminate or seriously reduce access to market prices by attacking price signals themselves. With communication networks damaged and online marketplaces taken down, access to relevant prices of goods and services is seriously hampered. Furthermore, the destruction of data can destroy knowledge of past, present, and future customers. Wiping data can destroy existing contracts, further leading to a breakdown of a market. The notPetya attack serves as an example of this phenomenon. In the attack Maersk temporarily lost nearly all of its shipping logs, nearly destroying its knowledge of existing customers. Online vendors affected, often were forced offline, limiting consumer access to prices on the market. In addition, longer term disruption of shipping would have reduced the division of labor by seriously hampering international trade. Nonetheless, markets have shown resiliency in responding to cyberattacks.

Markets are capable of rapidly transitioning to substitute goods and services. With their international logistics network offline, Maersk employees resorted to using personal emails, texting, and handwritten notes to communicate with clients and manage the logistics of international shipping while the specialized computing software was out of commission (Greenberg 2018). Furthermore, shipping companies unaffected by the attack were able to adjust their prices according to the sudden drop in supply of shipping services. Nonetheless, notPetya seriously impacted international trade for several days. Finally, the market is recognizing the

need for increased cybersecurity. Data shows that the cybersecurity business is on pace to double in the next five years (Stanton 2018).

6. Conclusion

Cybersecurity poses a unique challenge to both government attempts to provide security and market provisions of cybersecurity. Policy makers must balance their mandate to provide for the common defense with economic realities regarding the provision of cybersecurity. The bulk of the United States' cybersecurity defenses are private. Therefore, policy makers desiring a more secure cyberspace for Americans should recognize that cybersecurity cannot be provided by the same means as conventional security. Instead, policy should be directed towards recognizing potential cyberthreats abroad, minimizing potential externalities, minimizing moral hazards and perverse incentives, removing roadblocks to the development of superior cybersecurity methods, and achieving a clearer understanding of definitions in the realm of cybersecurity and cyber defense.

Works Cited

BII. 2016. “This One Chart Explains Why Cybersecurity Is so Important.” *Business Insider Inteligence*. https://www.businessinsider.com/cybersecurity-report-threats-and-opportunities-2016-3 (December 4, 2018).

Coyne, Christopher, and Peter Leeson. 2005. “Who's to Protect Cyberspace.” *Journal of Law, Economics, and Policy*.

Department of Homeland Security. 2018. “Critical Infrastructure Sectors.” *DHS*. https://www.dhs.gov/cisa/critical-infrastructure-sectors (December 4, 2018).

Fruhlinger, Josh. 2017. “Petya Ransomware and NotPetya Malware: What You Need to Know Now.” *CSO Online*. https://www.csoonline.com/article/3233210/ransomware/petya-ransomware-and-notpetya-malware-what-you-need-to-know-now.html (December 2, 2018).

Greenberg, Andy. 2018. “The Untold Story of NotPetya, the Most Devastating Cyberattack in History.” *Wired*. https://www.wired.com/story/notpetya-cyberattack-ukraine-russia-code-crashed-the-world/ (September 20, 2018).

Jensen, Eric Talbot. 2017. “The Tallinn Manual 2.0: Highlights and Insights.” *Georgetown Journal of International Law* 48.

Meyer, David. 2018. “Russia Blamed for 'Costliest Cyberattack in History'.” *Fortune*. http://fortune.com/2018/02/16/russia-notpetya-cyberattack-damage/ (December 2, 2018).

Mises, Ludwig Von. 1922. *Socialism: an Economic and Sociological Analysis*. Indianapolis: Liberty Fund.

Mises, Ludwig von. 1949. Mises Institute *Human Action: a Treatise on Economics*. Indianapolis, IN: Liberty Fund.

O'Connor, Fred. 2017. “NotPetya Still Roils Company's Finances, Costing Organizations $1.2 Billion in Revenue.” *Cybereason*. https://www.cybereason.com/blog/notpetya-costs-companies-1.2-billion-in-revenue (December 2, 2018).

Olenick, Doug. 2018. “NotPetya Attack Totally Destroyed Maersk's Computer Network: Chairman.” *SC Media*. https://www.scmagazine.com/home/security-news/ransomware/notpetya-attack-totally-destroyed-maersks-computer-network-chairman/ (December 1, 2018).

“Securing a Common Future in Cyberspace.” *World Economic Forum*. https://www.youtube.com/watch?time_continue=491&v=Tqe3K3D7TnI (December 2, 2018).

Singer, P. W. 2014. *Cybersecurity and Cyberwar: What Everyone Needs to Know*. New York: Oxford University Press.

Smeets, Max. 2018. “The Strategic Promise of Offensive Cyber Operations.” *Strategic Studies Quarterly*12(3).

Stanton, Samuel. 2018. “National Security” Grove City College.

USAF College of Aerospace Doctrine, Research and Education. 1997. “Three Levels of War.”

Wheeler, Tarah. 2018. “In Cyberwar, There Are No Rules.” *Foreign Policy*. https://foreignpolicy.com/2018/09/12/in-cyberwar-there-are-no-rules-cybersecurity-war-defense/ (November 4, 2018).