Cybersecurity as a Public Good

Harry Brown III

University of Maryland University College Graduate School of Science and Technology
Abstract

This brief exploration discusses cybersecurity as a public good. The discussion does not present this notion in purely political terms, or through an extensive review of public goods and cybersecurity’s relationship to them, but poses brief arguments for cybersecurity as a public good, and as a function of its utility to the common good of the state’s citizens. Arguments are also made to suggest whether government should intervene in establishing and implementing cybersecurity policy and measures in the private sector, to what extent and forms should this intervention take, what role private industry should have, and how these considerations and the nexus with national security support the argument for cybersecurity as a public good.

Keywords: cybersecurity, regulation, government, private industry, cybersecurity policy, public good.
# Table of Contents

Cybersecurity as a Public Good .................................................. 4
Cybersecurity in the Context of Public Good ......................... 4
The Role of Government and Private Industry ...................... 5
Arguments for Governmental Intervention ............................ 7
Modes of Government Intervention ........................................ 10
Impact on National Security .................................................. 11
Conclusion .............................................................................. 13
Bibliography .......................................................................... 17
Footnotes ................................................................................ 22
Cybersecurity as a Public Good

This preliminary research poses the notion of cybersecurity as a public good in terms of its utility to society, the government’s role, and the role of private industry. While the scope of this discussion has many connections to many multidisciplinary domains, e.g. political theory, international relations theory, transnational issues, etc., the focus is more on three fundamental questions: should government legislate cybersecurity, what specific kinds of governmental intervention are necessary, and to what extent should government be involved. It is in this discussion that we find the basis for the argument of cybersecurity as a public good.

Upon the basis of these assertions, we further pose national security implications of governmental intervention\(^1\) in private industry, why the private sector should be involved, and the role that the private sector should have in establishing and implementing comprehensive cybersecurity policy. We then conclude that the establishment of cybersecurity policy and measures are indeed a public good, and offer a framework for governmental and private industry cooperation.

Cybersecurity in the Context of Public Good

The public good is typically defined in the context of “shared benefits at the societal level” (Shergold as cited in Morrell, 2009a, p. 543), hence, cybersecurity as a public good suggests the body of instruments, legislation, standards, and otherwise, that contribute to the good of the public by securing computing and information resources\(^2\) for purposes from which society derives substantial\(^3\) benefit. Here we are discussing the Internet, computers, networks, hardware, and informational resources that comprise the electronic foundation upon which modern society has come to rely upon (which is also referred herein as cyberinfrastructure). It
would reasonably follow that the governance of the cyberinfrastructure would be an important consideration to ensure the perpetuity of public good in this regard. It is necessary to introduce this notion at the introductory stages of this discourse to ensure an adequate understanding of cybersecurity as a public good as we pose various arguments, motivations, and reasons for or against government intervention.

**The Role of Government and Private Industry**

Within the context of cybersecurity, government intervention would be actions taken by the government to improve and secure information resources and address cyber threats. These threats exist in the public, governmental, political, and military domains. Gordon Snow, Assistant Director of the Federal Bureau of Investigation, testified before U.S. Congress on cybersecurity threats and vulnerabilities posed to the general public, business sector, and international implications (Snow, 2010). These included: fraud tactics, exploiting the wave of social engineering, “Phishing scams,” establishment of cyber-criminal enterprises, and international crime rings specializing in cybercrime (Ibid). Threats and vulnerabilities are posed in other domains, such as critical infrastructure, governmental agencies (political), and military institutions. In regard to the critical infrastructure, the Industrial Control Systems Cyber Emergency Response Team (ICS-CERT) reports incident response for industrial control systems (systems that control critical infrastructure, e.g. energy, water, dams) to have increased by 2,100% (Industrial Control Systems Cyber Emergency Response Team., 2012, p. 2, Figure 1). The National Association of State Chief Information Officers (NASCIO) and Deloitte suggest that while there has been a general downward trend in malicious software, web, hackers, and physical attacks, there has been an increase in state-sponsored cyberattacks, as well as in cyber-
based financial fraud. The NASCIO state that given this trend, “emerging cybercrime and state-sponsored threats will require a strong response from states” (National Association of State Chief Information Officers and Deloitte, 2012, p. 17, Figure 12). While obtaining specific trend information on military cyber attacks proved difficult and beyond the scope of this research, current literature support the assertion that the incidence of military cyber attacks have increased substantially and become more directed. As early as 2000, as many as 1,400 cyber attacks on the U.S. military were reported (Homeland Security News Wire, 2009). In 2008 to 2009, more than 54,640 attacks are alleged to have been perpetrated against the U.S. Department of Defense (Ibid). In private industry, data breaches have increased by approximately 400% (McAfee Labs, 2012, p. 19, Graph "Data Breaches Made Public"), and as the testimony from the Assistant FBI Director suggest, cybercrime remains to pose a substantial threat in all domains. Considering that a huge part, if not most, of commercial enterprise is based on electronic transactions, that the electronic commercial infrastructure facilitates business to customer, business to business, and business to employee services, as well as E-Government services that “provide citizens, organizations, and other governmental agencies” with information and the means to carry out public services (Valacich & Schneider, 2012, pp. 142-184); that information, digital media, collaboration, and other interactions are based on the current cyberinfrastructure⁵, and our society has come to rely on these capability and resources, any disruption in or destruction of these public goods is not in the best interest of the state or its constituency. When considering how automation and control systems have been integrated into the critical infrastructure, any disruption could have devastating effects. As Volonio & Robinson state, “because computers and networking systems control power plants, telephone systems, and transportation systems, as well
as water and oil pipelines, any disruption in these systems could cause loss of life or widespread chaos” (as cited in Valacich & Schneider, 2012, p. 417). This is especially the case as these components may be specifically targeted by state-actors and terrorists.

These conditions suggest substantial threats that compel cybersecurity policy at the government level to secure the cyberinfrastructure upon which these public goods are based. Asllani, White, & Ettkin propose that this environment creates “a compelling need for a cybersecurity doctrine” given the current environment (2011, [Abstract]). The argument now is to what extent should this government intervention be allowed and implemented.

**Arguments for Governmental Intervention**

We have established that the government is compelled to implement cybersecurity policy for the public good. From a jurisdictional view, it is expected that good governance would require measures to secure its own agencies and operations, however, as indicated earlier, said public good extends beyond the governmental domain to private industry. Given the cybercrimes noted by the FBI Assistant Director and trends indicated, cybercrime poses tremendous threat to private industry, and the extent to which the private industry is vulnerable poses tremendous risks to social order and economic interests. To what extent should government intervene to secure computer and information resources in the private industry?

In the Congressional Quarterly Researcher, Ellen McCarthy (2010), President of the Intelligence and National Security Alliance, suggests that the government should “regulate cybersecurity,” but that it lacks the human capital, legal authority and policies needed to establish and lead the implementation of a massive cybersecurity program across all sectors.” McCarthy goes on to say that the more substantive issue is how much regulation is actually needed or
wanted by the private sector. Given the assertion that the government lacks the essential components for a cybersecurity program on a national level, the construct that McCarthy suggests is to allow private industry to lead the cybersecurity initiative and build cooperative institutions to facilitate the implementation of cybersecurity policy. From her argument, we may pose three primary components of government intervention: (1) an overarching policy established by the government to guide this process, (2) a working alliance through cooperative measures for the purposes of “providing indications and warnings of threats, share potential solutions and provide a clearinghouse for standards” (Ibid), and (3) an a cooperative organ to “provide shared situational awareness,” and serve as an “interface with the government in the development of regulation” (Ibid). A historical example of the latter component may be observed in the establishment of the North American Electric Reliability Corporation (NERC) in the 1960s, which provided similar oversight and administration in the energy sector.

This “soft” regulatory argument (McCarthy & Clinton, 2010) does bear merit, especially having a successful historical precedent; however, it may be argued that the NERC was successful because it addressed regulation in a single sector, not an all encompassing national program across all sectors.

In the same article, Larry Clinton, President of the Internet Security Alliance, argues that the current “federal regulatory model” is outdated and is not structured to address ‘21st century issues like cybersecurity’ (McCarthy & Clinton, 2010). He furthers that any regulation should address mitigating the effect of corporate wrongdoing on society. He suggests that mandatory standards would be focused on technical and operational issues that would serve more to stifle business with increased costs, ultimately having national economic repercussions. These
consequences would “harm both our economy and national security” (Ibid). Clinton’s solutions include government spurring investment and innovation in cybersecurity, and creating a social-contract model similar to that created to build the system for the universal telephone and power services over 100 years ago (Ibid).

While other arguments exist, those presented above likely fall within the mainstream of opinions. Within these arguments we may observe a tension unique to our democratic political system where the regulation of public good is constrained by free enterprise. As an example, one specific area where such constraints may be observed is in the area of privacy. Given the constraints between government and private enterprise, government is prohibited from imposing overwhelming regulation upon private enterprise, which, consequently places a burden on the private sector to secure computing and informational resources. The challenge is to mitigate these considerations with national security, as the cybersecurity threats posed to private industry could rise to the level of compromising national security. A part of this national security is a compelling national interest to ensure not only national security in terms of political and military threats, but to ensure social order and economic stability.

Thus, the most favorable solution lies in a *Laissez-faire* approach which includes elements of the soft regulatory framework proposed by McCarthy. Perhaps departing somewhat from the pure *Laissez-faire* approach, the suggested solution should be more assertive on the part of the government to provide incentives and motivations to private industry, and make certain that the recommended cooperation occurs, and alliances are built to bring about the desired outcomes. It may be argued that it might be appropriate for government to impose penalties where private industry fails to implement a baseline of cybersecurity measures. As part of the
soft approach solution, the private sector has a responsibility to play a significant role in both
regulatory and cooperative initiatives to implement effective cybersecurity policies for its part in
ensuring economic and social stability through securing economic and social components
discussed earlier (reference the latter part of The Role of Government and Private Industry).

Modes of Government Intervention

The goal of this research is not to propose new instruments for government intervention,
but to explore cybersecurity as a public good in respect to current legislation and policy
initiatives. Figure 1 identifies seven instruments by which government intervenes to implement
cybersecurity policy. While the governmental intervention in Figure 1 does not represent all
cybersecurity policies and instruments, it presents a large part of the government’s role in
establishing and implementing cybersecurity policy, and the governments most assertive efforts
to ensure the public good as described earlier. There are other regulations and statutes directed at
cybercrime in such areas as illegal distribution of intellectual property and child pornography,
however, these area lie outside of the cybersecurity as a public good within the context of
governmental regulation.

In addition to those instruments identified in Figure 1 and government’s responsibility to
ensure the public good, the government has a responsibility to protect. These instruments
provide the legal basis to protect computers and information resources, and “shields them from
trespassing, threats, damage, espionage, and from being corruptly used as instruments of
fraud” (Doyle, 2008, p. 1). More importantly, these measures protect citizens from domestic and
foreign threats, and preserve and defend those unalienable rights granted under the U.S.
Constitution, e.g. citizen’s right to be secure, government’s obligation for common defense and protect from invasion.

<table>
<thead>
<tr>
<th>Government Intervention/Regulation</th>
<th>Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>I  CNSCI</td>
<td>Cooperative</td>
<td>An initiative by the current administration to: ‘(1) establish a front line of defense against today’s immediate threats, (2) defend against the full spectrum of threats, and (3) strengthen the future cybersecurity environment’ (National Security Council, 2009). Primarily directed at governmental institutions with some initiatives directed to the private sector for supply-chain security and critical infrastructure.</td>
</tr>
<tr>
<td>II Computer Fraud and Abuse Act (CFRA)</td>
<td>Penal Code</td>
<td>Act prohibits “hacking of commercial computer systems... and intentionally accessing a computer without authorization and thereby improperly obtaining information from the computer” (as cited in Walecki, Walecki, 2006, p. 140).</td>
</tr>
<tr>
<td>III FISMA</td>
<td>Procedures</td>
<td>“The Federal Information Security Management Act of 2002 (FISMA), consists of Title III of the E-Government Act of 2002 (U.S. Public Law 104-347) enacted into law at the close of 2002. FISMA outlines a mandate for improving the information security framework of federal agencies, contractors and other entities that handle federal data (i.e., state and local governments). FISMA consists of a set of directives governing what security responsibilities federal entities have, and it outlines oversight and management roles to the implementation of those directives” (Moyle, 2006).</td>
</tr>
<tr>
<td>V National Cybersecurity Division of DHS</td>
<td>Collaborative</td>
<td>“The National Cyber Security Division (NCSD) works collaboratively with public, private and international entities to secure cyberspace and America’s cyber assets” (U.S. Department of Homeland Security (DHS), n.d.).</td>
</tr>
<tr>
<td>VI NIST</td>
<td>Standards Procedures</td>
<td>Governmental agency for standards and procedures, namely the Cybersecurity Framework created under the executive order of the President of the United States for “improving critical infrastructure cybersecurity” (National Institute of Standards and Technology (NIST), 2013).</td>
</tr>
<tr>
<td>VII RedRAMP</td>
<td>Evaluative Authoritative</td>
<td>“The Federal Risk and Authorization Management Program (FedRAMP) is a government-wide program that provides a standardized approach to security assessment, authorization, and continuous monitoring for cloud products and services” (U.S. General Services Administration (GSA), n.d.). FedRAMP is the approach implemented under FISMA for assessment and authorization of IT services.</td>
</tr>
</tbody>
</table>

**Figure 1.** Modes of Government Intervention/Regulation for Cybersecurity Policy.

**Impact on National Security**

The notion of cybersecurity as a public good within a regulatory context suggests those compelling factors that bear on the sovereign’s responsibility to establish, maintain, and protect that public good. This consideration has many connections with national security, especially
given the nature of cyberattacks and the rise of these incidents on government and critical infrastructure. The compelling motivations for government intervention are magnified when cybersecurity as a public good is not preserved and protected. If the current policy and initiatives for cybersecurity were not implemented, the vulnerabilities and threats to both governmental organizations and the private would increase substantially. In the event of an overwhelming cyberattack from a nation-state, terrorist group, or other source, the consequences could be economic, social, and political instability and chaos. The absence of cybersecurity would create an environment of uncertainty, where socio-economic and political conditions would be unpredictable. Such an environment would be indicative of “diminished consumer demand, a reduction in resources and services, and ‘the ease with which business is conducted’” (Brown III, 2005, p. 33; Czinkota, Knight, & Liesch, 2004). Depending on policy implementations, such an environment might be created where only the minimum cybersecurity requirements are met on a broad scale.

On October 12, 2013, Leon Panetta, the Secretary of the Department of Defense described the affects of cyberattacks on two oil companies in Saudi Arabia (King, 2012). One attack succeeded in destroying data on as many as thirty-thousand computers (Ibid). Fortunately, the “primary corporate systems that handle[d] hydrocarbon exploration and production” were isolated from the systems affected (Ibid). An interesting and important factor about this attack is that it posed such great threat that the report had been classified by the U.S. government, subsequently to be declassified to “help the public understand the magnitude of the threat” (King, 2012). More importantly, Panetta suggested that the magnitude of this attack and its implications show that “a cyber attack perpetrated by nation states or violent extremist groups
could be as destructive as the terrorist attack of 9/11” and that such attacks rise to justify a military response (Ibid), indicating that such attacks are perceived as a serious threat to national security. These attack was an attack on a private corporation, which suggest that a large-scale attack against the business sector could have similar consequence. They could have been more devastating and likely disrupted the flow of oil in the region (PressTV, 2013; Reuters, 2012). National Security Agency Chief Keith Alexander states, “disruptive attacks that have hit almost every major American corporation from Google to AT&T will shift to a more ruthless variety” (Herridge & Press, 2012). These trends, the nature of the attacks, and threat potential show a substantial connection between the private industry and national security. This also supports earlier assertions of the uncertainty and instability that would likely result from these kinds of attacks, which are on the rise (Herridge & Press, 2012; Protalinski, 2012). Similar attacks and implications may be observed in the attack on: the Pentagons systems, Lockheed Martin (a U.S. Defense Contractor), the Georgian government during the Russia-Georgian war that began in 2008, Iran’s nuclear facility computers and centrifuges (Baldor, 2011; Gorman & Barnes, 2011; Wyler, 2011). This is a small set of known cyberattacks, however they suggest a significant and increasing threat to national security. It is through these notions and realities of the current cyber threat environment, that a strong relationship exists between cybersecurity policy and the public good.

**Conclusion**

The notion of cybersecurity as a public good implies many aspects of cybersecurity policy in relation to its impact on society. Whether that policy should be a function of governmental intervention through regulatory measures or cooperation has been a major part of
our discussion. From the arguments posed, government intervention is both a requirement and an obligation, and it is to a major extent and for the public good that government should guide cybersecurity governance, implement policy, and ensure the implementation of effective cybersecurity measures by private industry. Government has implemented cybersecurity policy through both regulatory and cooperative instruments; however, it appears that policy might be more effectively formulated by a central cooperative organ for cybersecurity governance. This central commission would bring clarity and bring order to the many initiatives that have been created for cybersecurity policy and measures in the private sector. Having private industry lead in the comprehensive cooperative initiative (and even be involved on statutory development) will remove traditional roadblocks of government and provide industry driven processes for the development of policy, requirements, standards, and monitoring.

Finally, in the current environment, cybersecurity threats posed in the governmental and private domains are such that they can compromise national security. Both government and private industry have a substantial role to ensuring comprehensive and effective cybersecurity as the threats increase and grow in magnitude. Consequently, weak cybersecurity policy poses a threat to the public good. Considering that attackers will continue to be persistent and find new ways to exploit cyberspace and attack government and private targets, the implementation of moderate cybersecurity measures will only protect from moderate cyberattacks. Institutions must be relentless in fortifying their computing and information resources by implementing strong cybersecurity policy. This will maximize utility for government, private industry, and citizens. Figure 2 represents this utility or public good as a function of cybersecurity policy.
These conditions and considerations render cybersecurity as a public good that is essential for our society.
Figure 2. Cybersecurity as a function of Public Good

Public Good = f(Cybersecurity Policy)
Bibliography


direct=true&db=poh&AN=43460552&site=eds-live&scope=site


Footnotes

1 It should be noted that while the *intervention* is often used as an international relations terms for the use of force in conflict, it is not used within that context here. It is meant to suggest the activities through regulatory or other measures that span from the government imposing requirements upon private industry to cooperative engagements that are implemented.

2 Information resources includes software, networks and other hardware, combinations thereof, information and management of these components.

3 ‘Substantial benefit’ is used here because within the theoretical discussion of public good, the absence of the component contributing to the good of society would actually be harmful to society (Morrell, 2009b, pp. 542-546).

4 It is assumed that the reader is familiar with the cybercrimes noted by the Assistant FBI Director Gordon Snow. These crimes have either shown to have become more persistent or more harmful to the general public in the form of identity theft, financial fraud, and other crimes perpetrated through data mining and organized cybercrime (The Federal Bureau of Investigation., n.d.).

5 The term Cyberinfrastructure embodies those computing and information resources that make up the networks, software, middleware, hardware, rules, standards, and human resources that facilitate all activity on the Internet (cyberspace). Such a notion may be localized, but not necessarily bounded, within a jurisdicational context.

6 While there might be a nexus between the ‘responsibility to protect’ in an international law context and the responsibility of a state to protect its citizens by social contract, it should not be confused here with the international law proposition that “states have a responsibility to protect their own populations from mass atrocities” (Glanville, 2012). It is extended here from the argument that a state has a social obligation to protect its citizens by preserving and providing public goods, which if retracted would result in harm to its citizens.