Chapter 3

# GOVERNMENT INTERVENTION IN INFORMATION INFRASTRUCTURE PROTECTION

Dan Assaf

**Abstract** Critical information infrastructure protection is the subject "du jour." An important part to addressing the issue is to answer the question whether the private sector or the government should be responsible for protection. The choice of governing arrangement – government provision, private provision or any combination thereof – is essential to ensuring an adequate level of security. This paper discusses how the market for critical information infrastructure protection may be susceptible to various market failures, namely public goods, externalities and information deficits. The presence of these market failures suggests that government intervention in the market is necessary. While this paper does not present a specific regulatory model or a set of regulatory tools to address these market failures, it asserts that understanding the market failures inherent in critical information infrastructure protection is a key element to designing a successful regulatory policy. Failure to understand and acknowledge the reasons for the inability of the private sector to provide adequate protection can impact a nation-state's security and render it vulnerable to attack.

**Keywords:** Critical information infrastructure protection, cyber security, market failures, government regulation

## 1. Introduction

Critical information infrastructures (CIIs) have become viable targets for adversaries, and it is extremely important to secure them in order to mitigate the risk from information warfare attacks. In the United States, as well as in other developed countries, most critical infrastructure assets are owned and operated by the private sector. As markets around the world undergo liberalization and privatization, the private sector is rapidly increasing its ownership of critical infrastructure assets in developing countries. With this in mind it

could be inferred that the market should be left to its own devices to provide critical information infrastructure protection (CIIP). However, there are certain instances when the government should intervene in the market. One instance is when the market cannot provide or under provides the good it is supposed to provide, a phenomenon referred to as "market failure" in neo-classical economic theory. Another is when the government intervenes in the provision of the good (although the market can provide the good) due to paternalism or based on values such as distributive justice or corrective justice.

While the protection of CII assets is an essential part of a country's national security efforts, the potential targets are usually private companies. But companies are self interested by nature, pursuing business objectives such as the maximization of profits and shareholder value instead of public values such as national security. This raises some interesting questions. Should the government intervene in the provision of CIIP although this negates the market-based approach of non-intervention? Should the government leave a national security issue – where a failure could have catastrophic consequences – in the hands of self-interested private firms?

This paper sheds light on the nature of the market for CIIP. It examines whether there is a need for government intervention. The analysis provides a possible answer to why the American policy of endorsing a "hands-off" approach and keeping faith in the market has been ineffective so far [2]. The market for CIIP has characteristics that indicate market failures, specifically, public good characteristics, presence of externalities and informational problems. These market failures call for government intervention to correct them. Furthermore, the market failures are cumulative. This point is key as it affects the choice of remedy – regulatory tools that address market failures.

The following section discusses the free market notion and the limited role that government should play in it under neo-classical economic theory. Next, the neo-classical economic justifications for government intervention are highlighted and applied to CIIP. Finally, the paper asserts that a new model is required to govern CIIP, one that calls for a more active role for the government. While a specific model is not presented, the paper stresses the importance of understanding the nature of the market for CIIP in the analysis of solutions.

## 2. Role of Government in a Market Economy

Neo-classical economic theory, based on Adam Smith's classical notion of the Invisible Hand [18], suggests that government intervention is required only when market failures are present. In other words, a market failure must be demonstrated in order to justify intervention.

Market failures that are most commonly demonstrated include monopolies, public goods and asymmetric information. More than one failure can be present in a market at the same time. For example, a market can be subject to the presence of both public goods and externalities [19]. Any of these market failures can justify government intervention.

# 3. Public Goods and CIIP

A public good is a phenomenon whose presence may demand government intervention in the market. It has two distinct, albeit related, characteristics. First, it is non-excludable; second, it is non-rivalrous in consumption [16]. Typical examples of pure public goods are clean air, radio broadcasts, street lights and national security.

When a good is non-excludable, either it is impossible to exclude non-payers from using it, or the costs of excluding non-payers are high enough to deter a profit-maximizing firm from producing that good. Non-rivalrous consumption means that the consumption of the good by one individual does not affect the ability of any other individual to consume it at the same level. Non-excludability and non-rivalry in consumption lead to a distorted outcome: consumers refrain from paying for the good and become free-riders. Thus, the market is not likely to produce and/or supply these goods and, when it does, it will do so in a sub-optimal manner. Government intervention is required to ensure the optimal production of these goods.

## 3.1 Is CIIP a Public Good?

Two propositions are central to justifying government intervention in CIIP on the grounds of public good: the national security proposition and the cyber security proposition. The first proposition is more intuitive and captures the essence of CIIP. National security is a (pure) public good; CIIP is an essential component of national security; therefore, CIIP should be regarded as a (pure) public good. The second proposition is less intuitive. Cyber security has some of the characteristics of a public good; therefore, the market for cyber security can be subject to failure. By itself, this proposition is unlikely to provide sufficient justification for government intervention.

## 3.2 National Security as a Public Good

National security is a classic example of a public good [12]. It is both non-excludable and non-rivalrous in consumption. Once it is provided, it is extremely difficult to exclude certain individuals from the security that is generated, and one individual's use of it does not detract from the amount consumed by others. This is the economic reasoning for the provision of this good by central government (there are other non-economic reasons for this as well). But what exactly is national security? Threats are no longer exclusively directed at nation-states. Corporations around the world are experiencing an escalation in threats and security incidents [11]. The new threats include information warfare, cyber crime and economic espionage, among others. The list of potential actors now includes terrorists, rogue states, hackers, competing corporations and international crime syndicates. The increasing reliance of public and private actors on information flow and information technology, which have led to

interdependencies between the public and private sectors, have contributed to the growth and evolution of these threats.

This situation has contributed to a change in what needs to be protected. In the past, national security involved protecting the nation-state and its institutions. Today, the definition of what needs to be protected is much broader, and it includes private entities whose activity is essential to a nation-state's economic and national security. Thus, the protection of CII assets is an important component of a nation-state's security, which, in turn, is a (pure) public good. Hence, it is important to include CIIP as an integral component of a national security strategy.

But the ability of the private sector to provide CIIP at an optimal level is questionable. It is likely that the private sector can provide protection at some level, perhaps at a level that protects its systems against criminal activity or unsophisticated industrial espionage. However, it is doubtful that the private sector can, on its own, protect against well-targeted information operations orchestrated by nation-states and terrorist groups. The private sector cannot provide an adequate level of security required to address sophisticated threats (for one, it cannot meet the high costs associated with an adequate level of security). This is a characteristic of a public good. Thus, the assertion that adequate levels of CIIP cannot be provided by the market, coupled with the adverse effects of inadequate CIIP on national security, calls for government intervention in the provision of CIIP.

## 3.3 CIIP as a Public Good

CIIP is a segment of what is generally known as cyber security (this is explicitly stated in Section 3(3) of the United States Cyber Security Information Act of 2000). Cyber security is considered to be a public good, although not a pure public good. It has strong public good characteristics – it is non-rivalrous in consumption and it generates positive externalities [7]. But it is not considered to be a pure public good because it is, at least to some extent, excludable.

One of the characteristics associated with the provision of public goods is the generation of positive externalities, which, in turn, leads to the creation of the free-rider problem. Therefore, the presence of positive externalities frequently points to the existence of a public good. Several scholars have addressed this concept in relation to cyber security. Jean Camp, for example, discussed the creation of positive externalities by the provision of security in a networked world [5].

The positive externalities in information security may be attributed to two sources. First, firms derive some benefits from other firms' reports of security breaches in their information systems and networks. The benefits include important information about attack methods, critical flaws in software that were exploited, etc. Second, there are positive spillovers from the actual implementation of cyber security policies and mechanisms by individuals or firms.

Consider the case of a distributed denial of service (DDoS) attack. If computer users adequately secured their systems, the chances of their systems being

used for DDoS strikes would be substantially lower. Hence, one user's security would generate positive benefits for the entire community. While the public enjoys increased security, the first users do not fully capture this benefit and, therefore, do not have an adequate incentive to protect their computers.

Powell models this as a prisoner's dilemma game and shows that, without coordination, users would make an inefficient decision (i.e., not secure their computer systems) [14]. Powell argues that cyber security is not a pure public good. He analyzed various surveys taken in the financial services industry, examining how businesses in the sector protected themselves against cyber terrorism. This included information about the investments made by companies in cyber security, their concerns about providing security, and whether they used security protocols. Powell concluded that "there must be enough of a private return to cyber security to cause firms to invest so much in it," and, hence, the market for cyber security is not failing.

Powell's conclusions are controversial for several reasons. An argument can be made, for example, that the financial services industry is not a good exemplar for the incentive structure related to investments in cyber security, because the benefits it derives from security investments are high relative to other critical infrastructure sectors. This is because the financial services sector relies heavily on online transactions and on maintaining consumer trust, which could easily be lost due to a security breach. Moreover, the threats that financial institutions defend against are not necessarily the same as those that chemical facilities face. Financial institutions are also very good at quantifying monetary losses and have experience in "return on investment" calculations for cyber security.

But even if we accept Powell's conclusions, they only point to the importance of distinguishing between the two propositions discussed above. More importantly, they point to the need to give more weight to the national security proposition. By failing to acknowledge this distinction, scholars risk oversimplifying the threats to CIIs. Upon considering the cyber security as a public good proposition alone, the conclusion that the market is working may seem quite plausible. However, after the national security proposition is added to the equation, the uncertainty disappears. Arguing for government intervention on the grounds that cyber security is a public good seems to be somewhat less convincing than arguing for intervention on the grounds that CIIP is a part of national security, and is thus a public good. This is why it would probably be harder to convince decision-makers to intervene in the general market for cyber security than it would be to convince them to intervene in the market for CIIP.

## 4. Negative Externalities

The second market failure identified by neo-classical economic theory is the presence of externalities in the market. An externality occurs when a decision by one actor in the market generates benefits or costs for other actors, which are not taken into account by the externalizing actor when making the decision. Externalities could be either positive (generating benefits) or negative

(generating costs). Consequently, market demand and/or supply are distorted, leading to socially inefficient outcomes.

A common example of a negative externality is a factory that pollutes the air in its vicinity. The pollution is a cost conferred on the people living nearby, a cost which the factory (and its end consumer) do not fully incur. When making the decision about the optimal quantity of goods to be produced, the factory's executives do not take into consideration environmental costs, and an above-optimal, inefficient quantity is produced. If the factory were required to internalize the costs conferred on its neighbors, it would not produce the same amount of goods.

According to the Coase Theorem [6], externalities can be avoided or corrected if voluntary exchanges take place. Coase asserted that where transaction costs are negligible, a voluntary exchange will take place and externalities will be internalized without the need for government intervention. In the polluting factory example, the factory and its neighbors would reach an agreement imposing the costs on the party that could internalize them in a least-cost manner. That is, if the costs generated for the neighbors were higher than the benefits derived by the factory from polluting, the neighbors would pay the factory to stop polluting. If the benefits derived by the factory were higher than the costs generated for the neighbors, the factory would pay the neighbors to relocate. However, as negligible or zero transaction costs are very rare, most parties affected by an externality cannot reach an agreement and government intervention may be warranted.

Justifying government intervention in the market for CIIP on the grounds of externalities seems intuitive, as discussed below. First, however, it is useful to discuss the important concept of interdependencies in critical infrastructures [15]. The term critical infrastructure interdependency emphasizes the correlation existing between the state of one infrastructure and the state of another. Power grids, telecommunication networks, banks, transportation, etc. are all interdependent. Thus, an attack on a communications network may have a debilitating impact on a power grid and vice versa. The fact that critical infrastructures rely on other critical infrastructures means that a disruption of one could lead to cascading failures in other critical infrastructures [20].

Following the notion of interdependency, a cyber-interdependency occurs when an infrastructure's operability relies on its information systems. Computers and automation systems are indispensable to operations in every critical infrastructure. Failure of information systems would lead to a failure of practically every critical infrastructure.

Thus, interdependency is a striking characteristic that leads to the phenomenon of externalities. Consider the case where executives of an Ontario-based energy company, which supplies all the electricity to Toronto, have to determine the level of security in their information systems. The chief information security officer (CISO) presents them with two options that differ in the level of investment required: (i) high-level security measures that would cost the company 0.5 million dollars and provide a 70% probability that the

*Table 1.* Total expected cost for high and low security levels.

| Level of Security | Cost of Security | Probability of Breach | Cost of Breach | Expected Loss | Expected Cost |
|---|---|---|---|---|---|
| High | \$0.5M | 0.3 | \$1M | \$0.3M | \$0.8M |
| Low | \$0.0M | 0.7 | \$1M | \$0.7M | \$0.7M |

company's information systems would not be breached; and (ii) very basic, free security measures, which only provide a 30% probability that the company's systems would not be breached. If the losses that the company would incur from a security breach are estimated at 1 million dollars, the decision that the executives face naturally involves some uncertainty. The uncertainty deals with the likelihood of a security breach. Under rational decision-making, the executives would compare the expected utility of each of the options presented to them.

The data and expected costs for the company are summarized in Table 1. Clearly, under a profit maximizing assumption, the executives would opt for the second strategy – a lower and cheaper level of security. It is not worth it for the company to invest more in security. Therefore, upon applying a cost-benefit analysis, the executives would choose the option that maximizes the company's bottom line.

This is where the externalities problem arises. The executives only took into account the expected loss to their company. They disregarded the interdependencies that exist between their company and other critical infrastructures – that a security breach in their information systems would spill over to other critical infrastructures and negatively influence their operations, inflicting losses on them. These additional losses did not factor in the cost-benefit analysis.

This conclusion is further strengthened by Kunreuther and Heal [10], who show that in an interdependent security problem where one compromised agent can contaminate others, investment in security can never be a dominant strategy if its cost is positive. The lack of incentive to consider the influence on other interdependent stakeholders underlines the need for government intervention.

The problem of negative externalities is not unique to CIIP; it also applies to the broader discipline of cyber security. When one decides not to install security software on one's computer, one puts one's own computer at risk as well as numerous other computers, because an unsecured computer could be used as a "zombie" in DDoS attacks. Externalities are, therefore, a problem inherent to CIIP and to cyber security in general. This supports the need for government intervention.

## 5. Information Deficits and CIIP

One of the basic assumptions underlying competitive markets is the availability of full or perfect information, or, at least, the availability of information

required to make choices between alternatives. Therefore, the third justification for government intervention in a market is the presence of imperfect or asymmetric information [13].

A simple example involving imperfect information is the used automobiles market, where sellers usually possess superior information regarding their cars than potential buyers. Information deficiencies can cause a market failure. In the used automobiles market, they may lead to an adverse selection effect – the crowding out of high-quality car sellers by sellers of low-quality cars (lemons). The result is a "market of lemons" – a market comprised solely of low-quality cars [1]. Akerlof [1] discussed several possible solutions to the problem of information asymmetry, all of which are based on the private market. However, in some circumstances, there is a need for government intervention to correct a failure and induce more efficient exchange.

The application of informational problems to CIIP (and cyber security) is somewhat counterintuitive, mainly due to the reduction in information costs in the Internet era [9]. However, the reduction in information costs is not pertinent in the context of cyber security and, more precisely, to the market for CIIP. One of the most important elements of cyber security and CIIP is information flow between all stakeholders: owners of critical infrastructure assets, state agencies, and other entities (e.g., US-CERT) who share information about flaws, threats and vulnerabilities.

The informational problem in the market for CIIP is that private owners of critical infrastructure assets are reluctant to share important security information with other owners and with the government. Thus, information is not shared optimally by all the stakeholders.

There are a number of reasons for the reluctance of stakeholders to share information with their counterparts. On the horizontal axis (i.e., among critical infrastructure owners), companies are reluctant to share information that may constitute valuable intellectual property. Also, there is a concern that released information could be manipulatively exploited by competitors (e.g., a competitor could pass certain information to the media to damage the company's reputation).

Consider a scenario involving the CISO of an American bank who discovers that a security breach in the bank's information systems has resulted in the theft of data about millions of customers. The breach was due to a security flaw in software used by almost every American bank. The "right" thing to do on the part of the bank is to report the incident (including the vulnerability that enabled the breach) to other bank CISOs and to the regulator. All the other banks could then fix the flaw and, thus, enhance the security of their computer systems. However, the benefit to the other banks entails a potential additional loss to the first bank. The other banks could pass information about the breach to the public, severely damaging the reputation of the reporting bank, leading to loss of clients and, ultimately, loss of business [17]. Clearly, the fear of losing its reputation would play an important role in the affected bank's decision about sharing the information.

On the vertical axis (i.e., between critical infrastructure owners and the government), information sharing is also flawed. The private sector is hesitant to share information with the government for several reasons. First, companies fear that information disclosed to the government will find its way to the public or, even worse, to competitors because of freedom of information laws. Some countries, including the United States and Canada, permit special exemptions to these laws for information regarding critical infrastructures that is shared with the government, but the problem of trust has not been resolved. Second, any leaks of this information could result in civil suits against companies for negligence. Third, companies fear that sharing information with the government could result in increased regulation. In particular, disclosures may induce the government to set security standards and regulations that could prove rather costly [4].

Similarly, the government should provide the private sector with valuable information (usually intelligence information) concerning cyber security. However, the government's inclination to maintain secrecy by classifying information, and to share information on a very narrow, need-to-know basis do not allow for efficient sharing [8]. Analogous to the incentives underlying information sharing between industry actors, security agencies tend to believe "that the risks associated with disclosure are greater than the potential benefits of wider information sharing" [8]. In economic terms, it seems that the government feels that the marginal costs of releasing the information are higher than the marginal benefits. This means that the optimal amount of information regarding the cyber security of critical infrastructures is not generated.

The reluctance to share information is quite costly. As Aviram and Tor [3] argue, sub-optimal information sharing can inflict social costs, especially in network industries, due to the fact that information sharing is crucial for compatibility, which in turn is a key component for producing positive network effects. The inability or reluctance of critical infrastructure owners to share information about vulnerabilities with other owners, along with the harsh consequences of attacks that exploit these vulnerabilities, produce immense social costs.

Indeed, the issue of information sharing on both the horizontal and vertical axes is not a clear case of information asymmetry, but rather a case of information deficit. There is not enough information available to all the stakeholders to enable them to make optimal choices on the basis of the information. This hampers the decision-making processes of the various actors, and leads to inefficiencies in the provision of CIIP. Consequently, there may be a case for government intervention.

## 6. Conclusions

The market for CIIP and, to a certain extent, the broader market of cyber security appear to be susceptible to a number of market failures, namely public goods, externalities and information deficits. The economic analysis presented is rather straightforward, but it sheds light on why the "hands off" approach

taken by certain governments in their policy toward CIIP has been largely ineffective in reducing the vulnerability of CIIs to attack.

Some market failures are remediable through voluntary, private action. But as we have seen, private action is sometimes ineffective. The presence of three market failures in the market for CIIP suggests that government intervention in the market is necessary. There are instances when government intervention could be limited in scope (e.g., when the regulatory instruments employed are more compatible with the market system). In other instances, collective action is required, and stronger regulatory intervention is warranted and is in the public interest. This paper has not presented a specific model, or a set of tools, for regulatory action. However, understanding the market failures inherent in the protection of CIIs is a key element in designing a successful regulatory policy. Failure to understand and acknowledge the reasons for the inability of the private sector to provide adequate protection affects a nation-state's security and renders it vulnerable to attack.

One point should be stressed. When advocating a new governing arrangement, arguing for regulation based on public goods, externalities or information deficits alone is insufficient as the regulatory tools used to remedy one market failure may not work on the other failures. Therefore, all three justifications for government regulation should be acknowledged, and integrated regulatory tools should be designed and put in place.

## References

[1] G. Akerlof, The market for "lemons:" Quality, uncertainty and the market mechanism, *The Quarterly Journal of Economics*, vol. 84(3), pp. 488–500, 1970.

[2] P. Auerswald, L. Branscomb, T. La Porte and E. Michel-Kerian (Eds.), *Seeds of Disaster, Roots of Response: How Private Action Can Reduce Public Vulnerability*, Cambridge University Press, New York, 2006.

[3] A. Aviram and A. Tor, Overcoming impediments to information sharing, *Alabama Law Review*, vol. 55(2), p. 231, 2004.

[4] L. Branscomb and E. Michel-Kerjan, Public-private collaboration on a national and international scale, in *Seeds of Disaster, Roots of Response: How Private Action Can Reduce Public Vulnerability*, P. Auerswald, L. Branscomb, T. La Porte and E. Michel-Kerjan (Eds.), Cambridge University Press, New York, pp. 395–403, 2006.

[5] L. Camp and C. Wolfram, Pricing security, in *Economics of Information Security*, L. Camp and S. Lewis (Eds.), Kluwer, Boston, Massachusetts, pp. 17–34, 2004.

[6] R. Coase, The problem of social cost, *Journal of Law and Economics*, vol. 3, pp. 1–44, 1960.

[7] C. Coyne and P. Leeson, Who protects cyberspace? *Journal of Law, Economics and Policy*, vol. 1(2), pp. 473–495, 2006.

[8] B. Crowell, Too many secrets: Overclassification as a barrier to critical information sharing, Testimony to the Markle Taskforce on National Security in the Information Age, Subcommittee on National Security, Emerging Threats and International Relations, House Committee on Government Reform, U.S. House of Representatives, Washington, DC (www.fas.org/sgp/congress/2004/082404crowell.html), August 24, 2004.

[9] N. Elkin-Koren and E. Salzberger, *Law, Economics and Cyberspace*, Edward Elgar, Cheltenham, United Kingdom, 2004.

[10] H. Kunreuther and G. Heal, Interdependent security, *Journal of Risk and Uncertainty*, vol. 26(2/3), pp. 231–249, 2003.

[11] R. Mandel, *The Changing Face of National Security: A Conceptual Analysis*, Greenwood Press, Westport, Connecticut, 1994.

[12] P. McNutt, Public goods and club goods, in *Encyclopedia of Law and Economics, Volume I – The History and Methodology of Law and Economics*, B. Bouckaert and G. de Geest (Eds.), Edward Elgar, Cheltenham, United Kingdom, pp. 927–951, 2000.

[13] A. Ogus, *Regulation: Legal Form and Economic Theory*, Clarendon Press, London, United Kingdom, 1994.

[14] B. Powell, Is cyber security a public good? Evidence from the financial services industry, *Journal of Law, Economics and Policy*, vol. 1(2), pp. 497–510, 2005.

[15] S. Rinaldi, J. Peerenboom and T. Kelly, Identifying, understanding and analyzing critical infrastructure interdependencies, *IEEE Control Systems*, vol. 21(6), pp. 11–25, 2001.

[16] P. Samuelson, The pure theory of public expenditure, *The Review of Economics and Statistics*, vol. 36(4), pp. 387–389, 1954.

[17] B. Schneier, *Secrets and Lies: Digital Security in a Networked World*, John Wiley, New York, 2000.

[18] A. Smith, *The Wealth of Nations*, Bantam Classics, New York, 2003.

[19] M. Trebilcock and E. Iacobucci, Privatization and accountability, *Harvard Law Review*, vol. 116(5), pp. 1422–1453, 2003.

[20] U.S.-Canada Power System Outage Task Force, Final Report on the August 14, 2003 Blackout in the United States and Canada: Causes and Recommendations, U.S. Department of Energy, Washington, DC (reports.energy.gov/BlackoutFinal-Web.pdf), 2004.