Who's to Protect Cyberspace?

Christopher J. Coyne
Department of Economics
Hampden-Sydney College
Hampden-Sydney, VA 23943
ccoyne@hsc.edu

Peter T. Leeson
Department of Economics
West Virginia University
Morgantown, WV 26506
pete.leeson@mail.wvu.edu

Abstract

Until now, the evolution of cyber security has been largely driven by market demand and has developed in the absence of formal governance. However, in the post-9/11 world and with an increase in cyber attacks, government's role in cyber security has become a major policy issue. This paper contends that economic principles have been excluded from the debate about who should provide cyber security. This paper seeks to fill this gap. We postulate that an analysis of cyber security in the absence of economic considerations is incomplete. Toward this end, we employ several economic concepts in order to offer insight to policymakers involved in this debate. In doing so, we hope to shed light on the most effective means of securing the Internet.

1. Introduction

Over the past decade, the growth of cyberspace has enabled individuals across the world to become increasingly connected. Table 1, which shows Internet access for different languages, highlights the extent of Internet expansion across borders and cultures:

Language	Internet Access (millions)	Percentage World Population Online	2004 (est. millions)
English	**262.3**	**35.6**	**280**
European Languages	257.4	34.9	328
Asian Languages	216.9	29.4	263
Total Non-English	**474.3**	**64.4**	**680**
Total World	**679.7**		**940**

Table 1: *Global Internet Statistics by Language (2003)*[1]

The development and expansion of the Internet has created innumerable new opportunities for access to information, personal interaction and entrepreneurial ventures.[2] Not only have the costs of communication fallen considerably but also, perhaps even more importantly, the sphere of potential trading partners has expanded

[1] Source: Global Reach (http://www.glreach.com/globstats/index.php3). Note that the "Total World" does not equal the sum of "Total English" and "Total Non-English". This discrepancy is due to an overlap between English and non-English figures. Many users access the Internet in two languages twice. The "Total World" row is lower than the sum to correct for this overlap. For more on the methodology see: http://global-reach.biz/globstats/refs.php3#overlap

[2] Varian et al conclude that the world wide web contains a textual content equivalent to that contained in 10 to twenty million books (McMillan 2002: 156).

dramatically creating immense new gains from exchange. Consider, for instance, the increase in eCommerce over the last four years, as illustrated in Table 2:

	2000	**2001**	**2002**	**2003**	**Estimated 2004**
Total $ (B)	$657.0	$1,233.6	$2,231.2	$3,979.7	$6,789.8

Table 2: *Worldwide eCommerce Growth*[3]

This is a tenfold increase over a four-year period. The online banking industry also highlights the increasing reach of cyberspace. The number of individuals using online banking services has increased 80 percent, from 13 million to 23.2 million, in the period from September 2001 to September 2003.[4] These rising trends illustrate the general fact that the lives of average citizens are becoming increasingly connected to cyberspace. This interconnectedness goes beyond direct interaction with cyberspace and extends to indirect interaction as well. Many of the services that the average individual relies on – water, electricity, mass transportation and other "critical infrastructure" – are linked to cyberspace although the end user may never realize it.[5] From direct interactions on personal computers and business networks to indirect interactions through critical infrastructure, the existence and development of cyber security is of the utmost importance for cyberspace to achieve its full potential.

Cyber security involves freedom from the risk of danger when interacting in cyberspace. As indicated, we consider participation in cyberspace to encompass a wide-range of activities including both direct and indirect interactions. Security takes on many

[3] Source: Global Reach (http://www.glreach.com/eng/ed/art/2004.ecommerce.php3)
[4] *Nashville Business Journal*, September 22, 2003 (http://www.bizjournals.com/nashville/stories/2003/09/22/daily5.html)
[5] The Patriot Act defines critical infrastructure as: "Systems and assets, whether physical or virtual, so vital to the United States that the incapacity or destruction of such systems and assets would have a debilitating impact on security, national economic security, national public health or safety, or any combination of those matters."

different forms in cyberspace including encryption techniques, firewalls, virus-scanning software, intrusion detection systems and secure payment systems. In the absence of security, the full potential of information technologies cannot be realized because users will be fearful of malicious activities (Cheswick and Bellovin 1994). From simple searches, downloads and communication on the Internet to more complex transactions, individuals require security for their hardware, software, personal information and online exchanges. In addition to the range of activities that require security, there is also a range of Internet users demanding a secure environment. These users include private individuals, businesses and government.

The increasing interconnectedness discussed above does come with the possibility of significant losses through cyber crime. For instance, in 2003, hacker-created computer viruses alone cost businesses $55 billion. This is nearly double the damage they inflicted in 2002 (SecurityStats.com 2004). In a 2004 survey by the Computer Security Institute (CSI), over half of respondents indicated some form of computer security breach over the past twelve months and 100 percent of respondents indicated a website-related incident over that same period (CSI 2004).

In the post-9/11 world, Internet security has become a major policy issue, specifically in the context of national security. Consider for instance the following from Tom Ridge, the former Director of Homeland Security:

> "When people think of critical infrastructure, they have a tendency to think of bricks and mortar…But given the interdependency of just about every physical piece of critical infrastructure, energy, telecommunications, financial institutions and the like with the Internet and the cyber side of their business, we need to be focused on both and will be…We [the government] need to do a national overview of our infrastructure, map vulnerabilities, then set priorities, and then work with the private sector to reduce vulnerabilities based on our priorities" (Quoted in Verton 2003: 235).

Who's to Protect Cyberspace?

One of our main aims in this paper is to provide a realistic understanding of how cyber security fits in with national security. Is it our contention that in the context of cyberspace, individual security, as it relates to each and every user, and "national security" are inseparable. Just as security at the personal level involves the absence of risk of danger, so too does national security. Indeed, neatly categorizing national security as its own distinct category, separate from cyber security is a difficult task. This is largely due to the fact that national security is directly dependent upon security at the lowest levels of cyber usage.

We often think of national security as a single good provided by government, national defense being one example. Cyber security, however, is distinctly different than this because at the national level it is simply the sum of dispersed decisions of individual users and businesses. Highlighting the role that individual users play, Verton writes, "Millions of home computer users with high-speed Internet connections fail to secure their connections, and become potential 'jumping off' points for terrorists and malicious hackers" (2003: x). The very essence of the Internet is interconnectivity. What this means is that national security concerns are directly linked to the most basic security issues that the average user faces.

In light of this, it is easy to see why cyber security is currently one of the main policy topics of discussion. The development of cyber security and growth of cyberspace in general has taken place with little central direction. According to its inventor, Tim Berners-Lee, the Internet grew "by the grassroots effort of thousands."[6] Currently, it is estimated that eighty percent of what is deemed "critical infrastructure" is privately

[6] *San Jose Mercury News*, January 30, 2001, books section, p. 2.

owned (Verton 2003: x). Potential problems arise, it is argued, specifically because of the Internet's decentralized nature. In short, no one user will be looking out for the national interest and hence national security. It is increasingly common nowadays to hear that the absence of coordinated efforts to protect cyberspace means vulnerabilities will persist. Given this, the conclusion often drawn is that the government must play an active role in protecting cyberspace against cyber crime and cyber terrorism.[7] The exact role that government is to take is still being debated.

As the title of this paper suggests, we focus on answering the question, "Who's to protect cyberspace?" Our core thesis is as follows: Although economic issues are at the center of cyber security, economic considerations have been largely absent from the policy debate. Economics can contribute to adjudicating between the various courses of action in determining policy toward cyber security. Toward this end we employ several basic economic concepts in order to offer insight to policymakers involved in this debate. In doing so we hope to shed light on the most effective means of securing the Internet.

Those in the legal profession have focused on governance issues related to cyberspace, which are closely linked to the issue of security. For instance, Johnson and Post (1996a, 1996b) postulate that since the Internet is not linked to any geographical polity, governance will take place via privately provided rules that lead to the emergence of common standards. Reidberg (1996) argues that the primary source of governance in cyberspace is technology developers. It is his contention that the hardware and software that allows users to operate in cyberspace imposes a set of default rules. Neither of these works, though, incorporates explicit economic analysis into their work. Our paper can be

[7] Pollit (1997) defines cyber-terrorism as: "The premeditated, politically motivated attack against information, computer systems, computer programs, and data which results in violence against noncombatant targets by subnational groups or clandestine agents."

seen as contributing to this discussion on governance, its new contribution being a focus on the economic aspects of cyber governance and security. There is also a growing body of literature in the area of the economics of information security (see for instance Anderson 2001; Camp and Lewis 2004). While the insights from this literature are extremely relevant to this debate, they have been largely neglected in both the private and policy realms.[8] Given this, and in light of increasing calls for government involvement in cyber security, it makes sense to highlight what economics can contribute.

This paper proceeds as follows. We first apply the economic concepts of marginal costs, marginal benefits and efficiency to the issue of Internet security. Section 3 discusses and applies the concepts of externalities and market failure to cyberspace. In light of this discussion, Section 4 highlights some ways that the market can overcome problems stemming from externalities. Section 5 considers the concept of government failure and the implications for government regulation of cyberspace. Section 6 discusses the policy implications stemming from our analysis. Section 7 concludes by reiterating the main points of our analysis.

2. Marginal Costs, Marginal Benefits and the Efficient Level of Internet Security

When considering any potential course of action, economists focus on weighing the benefits of the action versus its costs. More specifically, economists are concerned with the costs and benefits of undertaking an additional, or marginal, unit of the activity in

[8] See for instance, "The New Economics of Information Security," Information Week, March 29, 2004. Available at: http://www.informationweek.com/story/showArticle.jhtml?articleID=18402633 (last accessed 7/12/04).

question. If there is a net gain, where the marginal benefits outweigh the marginal costs, the activity should be undertaken, the result being an economic improvement. Likewise if the marginal costs outweigh the marginal benefits, the activity in question should not be undertaken. Economists refer to a situation as efficient if all possible improvements have been made such that no further improvements are possible.

The logic of efficiency has clear implications for cyber governance and security. If asked, most people would say that the optimal level of cyber breaches is zero.[9] But economics tells us otherwise. From an economic standpoint, what we want is the *efficient level* of cyber breaches. 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. Ultimately, what this means is that the efficient level of cyber breaches is not necessarily zero. For instance, if it costs $1 million to prevent a virus or cyber attack that only causes $500,000 worth of damage, the prevention should not be undertaken. In this example, the costs of prevention outweigh the benefits, and it is an efficient cyber breach.[10] We now have a general economic rule for considering the efficient level of computer security. Security efforts should only be undertaken if the marginal benefits outweigh the marginal costs. In general, the efficient level of cyber breaches is where the marginal costs of prevention exactly offset the marginal benefits of prevention.

---

[9] We use the term "breaches" here in the broadest possible sense to include such things as hacking, viruses, fraud, cyber terrorism, etc.

[10] There have been several attempts at measuring the costs of cyber breaches. See for instance, PricewaterhouseCoopers (2000).

In many cases, security efforts will be undertaken to prevent potential attacks, which may or may not in fact occur. For example, many of the current efforts undertaken by the government against cyber terrorism are done to prevent a potential attack from occurring. In such cases one can determine an expected probability that such an attack will in fact occur and calculate the expected cost and expected benefit of undertaking the security measure to prevent that attack from occurring.

The immediate implication of applying the basic concepts of marginal costs, marginal benefits and efficiency to cyber security is that the end goal of policy is not necessarily to reduce the level of cyber breaches to zero. Instead we should aim for a policy mix that yields the efficient level of breaches. Ultimately, what we want to achieve is a policy that sets the punishment for a breach equal to the cost of damage. If this can be achieved, only efficient breaches will be undertaken. In other words, those engaged in breaches will only commit breaches when the benefit they receive is greater than the cost (i.e., damage). Another implication is that considering only the aggregate number of breaches as a metric of the general cyber environment is not informative from an economic standpoint. The number of breaches tells us nothing about the cost they impose or the benefit of preventing them.[11]

The main difficulty with the cost-benefit approach is obtaining the relevant information to determine actual costs and benefits. This becomes even more difficult when attempting to perform this analysis on breaches that may or may not occur because this involves some degree of speculation, not only regarding the probability of a breach,

[11] For instance, part of the hacker subculture consists of hackers who breach a system and without doing any damage report the security holes to the system administrator. In this sense, they actually provide a benefit in repairing security holes before malicious hackers can take advantage of them. This benefit is not captured when one considers the total number of breaches and it is not clear that one would want to expend resources in preventing these breaches.

but also the damage it will cause.[12] As we will discuss below, the market is one means of generating the knowledge required for cyber security investments. Despite these difficulties, we now have a framework in place to judge the efficiency of security efforts.[13] One thing that is clear is that ignoring costs and benefits leads to an incomplete analysis and can potentially lead to wasted resources.

3. The Theory of Externalities and Market Failure

The notion of externalities is also extremely relevant to the discussion of cyber security. Economists define an externality as a net cost or benefit that an activity imposes on those outside (i.e., external to) the activity. The problem stemming from externalities is that an individual only considers the costs and benefits directly relevant to him. In other words, an individual's decision excludes the costs and benefits that the activity imposes on others.

Externalities can be either positive or negative depending on whether they yield an external benefit or cost. A common example of a positive externality is a scientific research breakthrough. In this case, the good produces a positive externality that has large spillover benefits to those outside the individuals actually engaged in the scientific research. In the case of positive externalities, the primary actor does not internalize all benefits of his action. Theoretically, positive externalities will be undersupplied on the market due to the free-rider problem stemming from non-excludability and pricing issues related to non-rivalry. One common example of a negative externality is pollution from a

[12] The efficient level of security has been debated by among others Anderson (2002) and Schneier (2002).
[13] It should be noted that there is software, for example CORA, which allows firms to calculate the return on a security investment. The software analyzes the costs of security breaches in terms of recovery time and weighs those costs against the benefits of investing in the prevention activity.

factory. In such cases, the primary actor does not internalize all costs of his action. Theoretically, negative externalities will be oversupplied because the producer will internalize all benefits of the activity but not all of the costs.

Externalities are said to lead to market failure because the market fails to efficiently distribute costs and benefits such that they are fully internalized. In other words, the market, left to its own devices, will fail to provide the incentives to produce the socially optimal level of goods with positive or negative externalities. The standard conclusion is that government must either be involved in producing the good or service, or must regulate the activity in question in order to align costs and benefits and to ensure externalities are internalized. In the case of negative externalities, government usually penalizes the behavior, while in the case of positive externalities it usually encourages the behavior through subsidies or other incentives.

Given the above rendering of externalities, we can now place cyber security within this context. First, it must be noted that the Internet produces what economists refer to as a network externality in that the value of each connection increases as the total number of connections increases. For instance, while one Internet connection may allow the user to search for specific information, the value of the connection increases as others begin to use the Internet as well. With more connections, there are more users to interact with, whether the purposes are commerce, information or entertainment.

Given the interconnectedness of cyberspace, the actions taken by users will spill over and affect other users. These spillovers can be either positive or negative depending on how we look at the issue. The failure to undertake security measures can potentially have large negative effects on other users. If two users are connected and one fails to

secure their system, he is putting the other user at risk as well. Likewise, security efforts undertaken by some users will provide a positive spillover to other users. To understand why, consider an analogy with vaccines. The prevention of communicable disease yields enormous spillover benefits to all members of a society. In other words, each member of a community benefits (i.e., receives a large positive benefit) if the other members of the community are vaccinated against a disease because they do not have to be concerned that they will catch the disease. A potential problem arises though because there is an incentive to free ride. If each individual believes that all others will be vaccinated, there is no reason for them to be vaccinated as well. The case with cyber security can be seen in a similar light. If everyone else's computer is vaccinated against viruses and protected against breaches, other members of the cyber community benefit as well and don't need to take steps to protect their system. For instance, those interacting with the uninfected user who regularly scans his computer do not have to be concerned with receiving a virus infection from that user.

As such, when individual users or businesses take steps to make their own computer or business more secure, they make the general cyber environment more secure as well, thus benefiting all users. Given this, economic theory predicts that individual decision calculus will yield too little security. The individual undertaking the security precautions does not internalize all the benefits, and will seek to free-ride off of the efforts taken by others. Similarly, when users fail to undertake security measures, they only incur part of the cost of their actions. Therefore theory predicts that security will be undersupplied on the market and vulnerability, or a lack of security, will be oversupplied on the market.

Who's to Protect Cyberspace?

Although not using the exact terminology specified above, policymakers often view cyber security within this framework. To illustrate this, consider the following quote from former Governor James Gilmore who led the Advisory Panel to Assess Domestic Response Capabilities for Terrorism Involving Weapons of Mass Destruction: "So far, pure public/private partnerships and market forces are not acting…to protect the cybercommunity. Relying on the private sector's willingness to do the right thing when it comes to security is simply not an answer" (Quoted in Verton 2003: 26). In economic terms, Gilmore is indicating that a market failure exists due to a lack of incentive on the unhampered market to "do the right thing" and provide the optimal level of cyber security. Indeed, the notion of externalities and market failure underlies all claims that the market will underproduce cyber security and that the government must intervene and regulate to makeup for the shortfall. Consider the following from Richard Clarke, the former cyber security czar:

> I went around saying that regulation was a bad thing because the government was stupid and would do it badly…But the thing about regulation is that there was always a footnote -- like, unless there's market failure, we don't want regulation. If the market doesn't cause voluntary processes [to change], then government gets involved.[14]

The immediate concern that results from issues of externalities and market failure are how these problem can best be remedied. There are at least two possibilities for dealing with the problem. One involves considering possible ways for the market to privately solve externality problems. The second is for government to intervene via regulation. In the next two sections, we treat each of these potential solutions in turn.

[14] Source of quote: "RSA: Can regulation cure security's ills?", available at: http://searchsecurity.techtarget.com/originalContent/0,289142,sid14_gci953148,00.html (last accessed 6/7/04).

4. Private Solutions to Externalities

Given that cyber security measures have large positive spillovers, economic theory predicts that these measures will be undersupplied on the market. The question then becomes whether economic theory's predictions are correct or if there are means through which the market can internalize the related externalities. Typically, there are several avenues through which goods possessing strong externalities can be privately supplied.

The key realization is that not all benefits have to be internalized for a good with externalities to be produced at the optimal level. Indeed, nearly every activity has some related externality. The good can be privately produced provided that there are solutions that allow *enough* of the benefits to be fenced off and internalized by the producer. Similarly, the presence of spillovers is itself not enough to prevent some producers from providing a needed good. Some producers may be motivated by good-will or act for other reasons unconnected to monetary rewards and therefore are willing to incur the cost of providing say, a public good, even though they gain little (or even lose) from a profit and loss perspective. In the following subsections we consider these two avenues through which goods possessing positive externalities are privately supplied in the context of cyber security.

4.1 Private Provision via Voluntary Donation

Voluntary donations are one method of funding goods with large positive externalities. Donations of money and artwork to museums, contributions to listener and viewer-

supported radio and television stations, and donations to health research all serve as some readily apparent examples. While economic theory would predict free-riding in such situations, we observe many individuals making such donations nonetheless.

There are several instances of the private provision of cyber security by the voluntary donation of time and/or money, completely separate from any government organizations encouraging this behavior. One example of this is CyberAngels, an organization that was founded in 1995 by Curtis Sliwa, head of the Guardian Angels. CyberAngles is a completely voluntary program whose goals include: (1) preventing online crimes through education, (2) assisting victims who have suffered from Internet crimes and (3) monitoring legal issues as they relate to the Internet across borders.[15] In line with these goals, the activities of the CyberAngels include searching for online fraud and scams, finding and reporting sites that use children in sexually provocative ways, monitoring children in child chat rooms, offering online classes and assisting victims of online harassment, stalking, fraud and hacking.[16] CyberAngels is funded through private donations from various donors ranging from individuals to corporations.

Microsoft's bounty program provides another illustration of the private provision of cyber security through private donations. In November of 2003, Microsoft announced that it was creating an anti-virus reward program backed by $5 million of its own cash. Under the program, a reward will be offered for information that leads to the arrest of the writers of computer viruses. The first two bounties announced were two $250,000 rewards for information leading to the arrest of the writers of Blaster worm and SoBig.F

[15] For more on the mission statement of the CyberAngels, see: http://www.cyberangels.org/mission/index.html

[16] The main website of the CyberAngels program (http://www.cyberangels.org/index.html) is available in four languages.

email viruses. Even more recently, Microsoft offered a $250,000 bounty on the creator of the MyDoom.B virus.[17]

The cases of CyberAngels and Microsoft's anti-virus reward program illustrate that while the free-rider incentive may indeed be present, it is not necessarily the strongest incentive. Other incentives such as good will, a feeling of civic duty or pride, or some notion of fairness or morality may be present as well. The key insight is that while it is appropriate for economic theory to assume a strict self-interestedness among the agents that populate its models, it is inappropriate to maintain that goods with large positive spillovers will not be supplied privately in the real world based on this assumption. While theory requires the simplification that reducing motivation to a single element entails, we must keep in mind that the world in which we find ourselves is considerably more complex and involves innumerable motivations that may completely outweigh the countervailing motivation of self-interest.[18] Clearly these donations are not, at their current levels, enough to protect cyberspace in its entirety. The main point though is that, contrary to theory, they do in fact exist. As the Internet continues to grow, there is no reason to expect that these types of voluntary donations will not increase as well.

---

[17] For details on this program see: http://www.microsoft.com/presspass/press/2003/nov03/11-05AntiVirusRewardsPR.asp

[18] Also of note is the market for "ethcial hackers" which are hired by companies to hack into their systems before "unethical hackers" can. Gartner Inc., a market research firm in Stamford, Connecticut, estimates this to be a $1.8 billion industry for the year 2002 with expected growth of 28% for the next three years. Some ethical hackers focus on one specific operating system such as eEye Digital Security (http://www.eeye.com/html/) that specializes in Microsoft Windows. In addition to assisting their clients, eEye voluntarily reports any holes in Windows to Microsoft, although they have no formal relationship, and doesn't publicly release the information on the security flaw until Microsoft develops a patch. See, Nick Wingfield, "It Takes a Hacker," *The Wall Street Journal*, March 11, 2002 and Brad Stone, "An eEye on Microsoft," Newsweek, March 22, 2004.

Yet another example of the private provision of cyber security through voluntary donation is open source code. Open source code has a long history in the development of the Internet. In its early stages, the Internet was a simple protocol for exchanging data. The early versions of this protocol included the file transfer protocol (FTP) and the electronic message protocol (SMTP). The subsequent development of the "Gopher" protocol allowed for directories to be depicted graphically. The hypertext transfer protocol (HTTP) and the hypertext markup language (HTML) were created in 1991 and are the foundation of the Internet as we know it today. These protocols were available to all users (i.e., open) and were used to develop many additional applications. Much of the subsequent software and applications developed were "open" – i.e., the source code and object code were available to all other users.[19] The rapid growth of the Internet has been attributed to this early openness of code (Lessig 1999: 103). Users could view the code of others and either improve or build upon it. In this regard, open source code can be seen as a good with significant positive externalities that is privately provided.[20] Individual users "donate" or allow for the code they developed privately to be open for all Internet users to view, copy and improve upon. Today, a mixture of open and closed code exists on the Internet. Nonetheless, open source code still plays a critical role in cyberspace and in Internet security.[21]

---

[19] Source code is the code that computer programmers write in. Object code is machine-readable (Lessig 1999: 103).

[20] Indeed, open source software would be an example of what economists call a pure public good. Once made public, it both non-excludable – all users can access it – and non-rivalrous – one users consumption of the code does not reduce the amount available for others. The notion of public goods and externalities are closely related. A public good possesses large positive externalities and a public bad large negative externalities. For more on open source code as the private provision of a public good, see James Besson, "Open Source Software: Free Provision of Complex Public Goods" available at: http://www.researchoninnovation.org/opensrc.pdf (last accessed 7/7/04).

[21] To support this claim, consider that the Apache system, the number-one server on the Internet, is open code as is SENDMAIL, one of the most widely used programs for forwarding email (Lessig 1999: 104).

Open source code relates to the issue of cyber security on two fronts. On the one hand, there are specific security programs based on open source code that are publicly available for downloading by all users. To a greater extent though, security is an issue with all open source code programs. With open source programs, the underlying code is available to all – both benevolent users as well as criminals. As a result, questions of security arise for open source programs given that all users have access to the code.

There is much debate regarding the viability of open source code from a security standpoint. Critics argue that open source code provides potential criminals with the blueprints of the security system. Advocates counter that the constant peer review actually makes programs based on open source code more stable and reliable as compared to commercial code. For instance, Vincent Rijmen, an award winning developer, believes that the open nature of Linux is preferable from a security standpoint, "not only because more people can look at it, but, more importantly, because the model forces people to write more clear code, and to adhere to standards. This in turn facilitates security review."[22] In any case, clearly all users of open source code receive a large positive spillover. Specifically, they gain a large benefit from the initial availability of the code as well as from improvements made to open source code by other programmers.

Another response to critics of open source security code is that those seeking security can take existing open source security code and make minor adjustments that customize the program specifically for the user. These adjustments can be open or closed code but the foundation is available through the initial open source code that existed from

---

During the first three years of Apache system's existence, 388 developers contributed 6,092 enhancements and corrected 695 bugs (Mockus et al. 2000). This rate clearly exceeds that of commercially provided software which relies on closed code (Mockus et al 2000, Table 1).

[22] Interview with Vincent Rijman, available at: http://www.linuxsecurity.com/feature_stories/interview-aes-3.html.

the work of others.[23] Several companies now offer security packages based on open source code including Guardent (http://www.guardent.com/), Covalent (http://www.covalent.net) and Astaro Corporation (www.astaro.com), to name a few.[24] In addition to the benefits discussed above, security based on open source code has the additional benefit of being lower cost, as the user does not have to pay licensing fees.

Open source software is clearly an example of a good with significant spillover effects that is nonetheless privately provided. Once it is written and the contribution is made available or "donated" to the cyber community, all users are able to access it and benefit. Although standard economic theory predicts that such goods will fail to be produced on the unhampered market, we observe the opposite. There are several potential incentives that lead to the provision of open source code. One is that those who make their code public benefit from others who improve on their initial code. There is also the potential for fame within the programming sub-culture.[25] While anyone can contribute by posting code, the reputation or fame mechanism serves as a sorting device for other users. Fame provides enough of a benefit for these programmers to provide code to the rest of the cyber community. Open source code has allowed for the continual innovation and development of new applications and programs. While there are both potential costs and benefits to using open source code, it is a clear example of a private solution to the production of a good with significant spillover effects.

---

[23] A survey by Franke and von Hippel found that over 19% of the firms who used the Apache system had modified the code while another 33% customized the system by adding on security modules obtained from third parties (2002). Indeed, it is because of the open source code that add-on modules have been developed. As of January 2004, there were over 300 modules developed. See http://modules.apache.org/.

[24] The U.S. Navy also uses an open source security program, SHADOW. See http://www.techweb.com/wire/story/TWB19981008S0010.

[25] On the issue of fame, see the *Economist* article, "An Open and Shut Case," May 10, 2001.

4.2 The Private Provision of Internet Security via By-Product

The free-rider problem can also be overcome if it is possible to tie a by-product to the externality. Television commercials are one example of this mechanism. Financing for commercial television comes mostly from private sponsors who pay for advertising to be aired during television programming. The by-product of the externality – here the television program – is the captive viewing audience. We see many analogous examples in cyberspace.

Many Internet applications offer security features free of charge, but tie in other features allowing providers to earn a profit. For instance, most free email applications (e.g., Hotmail, Yahoo mail, etc.) contain virus scan features that check incoming/outgoing emails and attachments for viruses. In order to benefit from these security features, users must register with the provider. The providers make profits through advertisers who target the users of the application. For instance, Hotmail members receive emails from sellers in their inbox. Yahoo offers a pop-up blocker free of charge, but the user must have an account and a companion bar is placed at the top of the Internet browser, providing links to other Yahoo services connected to advertisers.

In order to increase the number of users and garner profits from advertisers, these providers must make their products attractive. Because part of the attractiveness is security, producers offer this feature. Once again, security increases the value of cyberspace for all users. In this context, cyber security is privately provided because the captive audience has a value that advertisers are willing to pay for. As with advertisers on television, advertisers on the Internet are willing to pay to reach as many people as possible.

In a similar vein, some providers of security software offer one version of their application free of charge, but charge the user for an upgrade. They provide a basic level of security with no charge but include in the package advertisements for the premium versions of their software. A good example of this is Ad-Aware which is developed and distributed by Lavasoft.[26]

The Ad-Aware software erases spyware from a user's computer. Spyware is programming that is tied into downloads – often the user is unaware that it is associated with the download. Once downloaded, spyware uses the available Internet connection to send information from the user's computer to the spyware company. One form of spyware - commercial spyware - tracks the websites visited by the user. Commercial spyware is often associated with adware, which uses the information to send pop-up advertisements that fit with the information related to the user. A second and more dangerous form of spyware - domestic spyware - tracks and captures the activities of the user via their keystrokes. This form is analogous to a wiretap and sensitive information such as passwords and private email and instant messenger conversations are at risk (Mitnick and Simon 2002: 203-8). Ad-Aware scans the user's computer memory, registry and hard drives for commercial spyware components and allows for their safe removal.

While the basic version is free of charge, Lavasoft offers two other versions – Ad-Aware Plus and Ad-Aware Professional for a charge. These versions contain more features than the basic version. In this context, the positive externality is the free security software and the by-product is the captive audience that downloads the free version. The captive audience is enough in terms of potential profitability for Lavasoft to provide the

[26] For more on Lavasoft see: http://www.lavasoft.de/default.shtml.en.

basic version free of charge. There are other examples as well. For instance the basic version of ZoneAlarm, a firewall software product, is free of charge to any user. Similar to Ad-Aware, ZoneAlarm charges customers for more advanced versions of its software.

Internet security provided by most firms also falls into this category. Most businesses that utilize cyberspace invest resources in cyber security. It is in their interest to do so for several reasons. For one, as noted in the Introduction, breaches are costly. In economic terms firms should be willing to invest in cyber security up to the point where the costs are equal to the benefits. Moreover, consumers demand that their information and transactions be protected. In order to attract customers, online businesses must offer certain security measures. In the absence of minimal levels of security, we would expect the customer base of online firms to decrease significantly. The by-product of the externality – here cyber security, are the customers that are willing to offer the firm business. The key point is that these customers are willing to do so only if a secure environment is provided. The secure environment has significant spillover effects to parties outside the immediate transaction. Despite the fact that firms do not capture all of the benefits, they offer security because they secure enough monetary benefits through their direct interaction with customers providing them with business.

Consider for instance the case of formal online payment mechanisms such as PayPal and BidPay. These services allow buyers to make secure payments, via credit card or through their bank account, to sellers. Given that they are dealing with sensitive information regarding their customers, security is of the utmost importance. Given this, PayPal and BidPay make use of encryption technology to protect the information of their

customers – both buyers and sellers.[27] The services offered by these middlemen who provide payment mechanisms do provide significant positive externalities. As discussed earlier, the Internet is a network externality which increases in value the more others are connected and able to participate online. By providing the potential for secure transactions, these services increase the value of the Internet to other users by lowering transaction costs.[28] They provide security despite the fact that there are positive spillovers that they do not capture because it is the only way to maintain and increase their customer base and profitability.

Understanding that private businesses have an incentive to invest in Internet security is critical because the greatest fear for government agencies is that terrorists will breach the networks of critical industries and have significant negative spillovers on the economy as a whole. Given this, the key issue is whether these businesses will under-invest in security given that they don't internalize *all* of the benefits. Granted, they produce some cyber security as the numerous examples above illustrate. But the argument is that because of the externality, they will fail to produce the optimal amount. To remedy the problem, government often intervenes to either produce the good altogether or regulate the private production of the good attempting to overcome the market failure. We now turn to a discussion of the potential limitations of government's ability to effectively do this.

---

[27] Additionally, many of these payment applications offer insurance protection as well. For instance, PayPal has a "Seller Protection Policy," which protects sellers against fraudulent buyers, as well as a "Buyer Protection Program," which provides $500 of insurance coverage against fraud at no additional cost to the buyer.

[28] It is estimated that PayPal has 14 million subscribers. Source: http://www.wilsonweb.com/wct5/paypal_assess.htm.

5. The Theory of Government Failure

As discussed in Section 3, the theoretical rendering of externalities concludes that the privately optimal level will fall short of the socially optimal level. Government is often called upon to make up the shortfall through intervention and regulation. Policymakers calling for government to actively play a role in the provision of cyber security illustrates this. Fundamentally, their claims are grounded in the belief that the market will either altogether fail to supply Internet security or, where it does, will undersupply security. In many cases, theoretical academic research also concludes that the market will undersupply key elements of cyber security. For instance, the research of Gordon et al. (2003) concludes that security information sharing between firms will be sub-optimal due to the free-rider problem. One possibility, they conclude, is for government to subsidize the sharing of information between firms (2003: 479-80). However, just as economic theory suggests that there is the potential for market failures, it also indicates that there is a potential for government failures as well. Just as it is important to understand why the market may only imperfectly provide cyber security, it is equally important to appreciate why the government may fail to supply the efficient level. Therefore, considering the potential benefits of government involvement along with the related limitations and costs is of the utmost importance for an accurate analysis.

One potential option is for government to produce the good, either in conjunction with the market or instead of the market. The difficulty with this option stems from the issue of calculation. It must be realized that goods with significant externalities, just like all other goods, are not produced in one lump, but rather in marginal units. In the market, the profit and loss mechanism serves as the guide for determining the optimal number of

units to produce. Admittedly, it is true that where externalities exist, the profit and loss mechanism may not produce the same level as compared to a situation where externalities are fully internalized.

With government, however, the profit and loss mechanism is not just imperfect in the face of externalities—it is necessarily completely absent. This means that the state will never have any way of effectively determining the optimal supply of the good in question. In short, there is no way for any external party to calculate the optimal social stock of cyber security and, hence, to claim that it is over or undersupplied. To do so would require complete and perfect knowledge that one cannot possibly possess. It may be true that private businesses have difficulties calculating the exact return on investment (ROI) for security-related expenditures, but this will be even more difficult for government agents acting outside the profit and loss mechanism. Given this realization, while it is indeed possible that the government may provide more cyber security as compared to the private market, there is no reason to believe that it will provide the socially optimal amount. From an efficiency standpoint, it is not simply a question of the total dollar value of resources invested, but rather the allocation of those resources to their most highly valued uses. Calculating the optimal level of goods is far simpler using a theoretical model with simplified assumptions than it is in reality.

Yet another option is that government can choose to regulate the market production of the good in the hopes of internalizing the externalities. In the case of cyber security, this may involve regulating the specifications of hardware and software in order to internalize the externalities in the hopes of aligning costs and benefits and achieving

the socially optimal outcome. The main problem with this solution is the difficulty in gathering the relevant information necessary to effectively regulate.

For instance, the regulators must know and be able to assign the damage done by insecurities in cyberspace. Given the interconnectedness of cyberspace, these vulnerabilities may be difficult to track and assign to a specific user. Given that the regulator aims to align costs and benefits, in addition to knowing the damage done by vulnerabilities, he must also possess the relevant information regarding the costs of remedying the situation. This information will be difficult to obtain. It is in the interest of each user with vulnerabilities to convince regulators that the damage they are causing is lower than the cheapest means of correcting the problem. In other words, it is in their interest to convince regulators that the costs of prevention are greater than the benefits.

Yet another issue deals with the policy flexibility of regulators in the context of cyberspace, and more specifically with what legal scholar Michael Froomkin refers to as "regulatory arbitrage" (1997). Because cyberspace connects users across national boundaries, Froomkin argues it will become increasingly difficult for any one nation to enforce its domestic rules. In other words, users can engage in regulatory arbitrage and evade domestic laws by engaging with users outside their national borders who are not subject to the same laws.

Admittedly, government can take steps to impede the use and effectiveness of cyberspace. For instance, China has attempted to set up an Internet censorship system known as "The Great Firewall of China." While this effort has raised the cost of engaging in cyberspace, users have found ways around the barrier largely by using servers outside the firewall. In sum, one potential limitation on the government provision

of cyber security deals with constraints on flexibility stemming directly from the very nature and magnitude of cyberspace.

As was illustrated by the quotes from policymakers in earlier sections of this paper, one of the criticisms of the market provision of cyber security is that there is a lack of incentive to consider the national interest. However, it is critical to realize that there are perverse incentives in the political realm as well. As Ranum describes his research on the topic of homeland security: "I came face to face with the realization that there are gigantic bureaucracies that exist primarily for the sole purpose of prolonging their existence, that the very structure of bureaucracy rewards inefficiency and encourages territorialism and turf war" (2004: xv). Indeed, as public choice theory informs us, political agents face a set of incentives that are in many times misaligned with the interests of the populace.[29] The implications are clear: the presence of misaligned incentives in the market does not give one license to jump to the conclusion that government intervention is preferable. Instead, a complete consideration of potential government intervention must involve a consideration of the incentives faced by political agents and the implications of those incentives for the provision of cyber security.

A final constraint on government regulation of cyber security is the potential for limited control of the response to policies by the private market. When considering a potential regulation, due to genuine structural ignorance, only some of the potential costs, benefits and impact on incentives can be known *ex ante*. Once a regulation is passed, it creates a new set of incentives for both political and economic agents. In many cases, the outcomes that the new policy generates will not be aligned with the initial aim. This will leave government officials in a situation where they can either retract the original policy

[29] For more on the public choice research program, see Buchanan (2003).

or pass additional policies to attempt to solve the unintended outcomes. This limitation may be potentially magnified in the case of cyberspace for the reasons addressed above – namely the continually changing cyber environment.

6. Policy Implications: Internalizing Externalities

We have discussed the potential limitations in both the market and government spheres in the context of cyber security. Fortunately, in addition to providing insight into the limitations of the market and government, economics also provides specific guidelines for policymakers. From an economic standpoint, the market provision of goods and services is preferable to government provision. This is due to the fact that the profit/loss mechanism inherent in the market setting guides economic actors in allocating resources to their most highly valued uses. In the context of cyber security this means that policies should be aimed at taking advantage of the desirable consequences of the market. It is only through the market process that the "right" amount of cyber security can be produced. More specifically, policy should be focused on internalizing the externalities while maintaining the allocative function of the profit/loss mechanism. Recently, several alternative courses of action have been discussed that potentially serve to internalize externalities. In theory, these potential solutions allow the desirable aspects of the market to function while overcoming the potential pitfalls of direct government regulation.

One potential solution is the assignment of property rights. Well-established property rights result in markets incorporating the presence of externalities. Along these lines, one solution that has been proposed by Camp and Wolfram (2000) is the assignment of property rights to cyber vulnerabilities. This solution is similar to

proposals for tradable pollution permits. Camp and Wolfram not only provide a taxonomy of vulnerabilities but also propose a means of assigning property rights. They propose that each machine would receive a certain number of vulnerability credits. Processing power is suggested as a measure of how many machines, and therefore how many credits, are to be received.

The authors suggest three potential governance mechanisms to oversee this process: the federal government, the creation of a corporation similar to The Internet Corporation for the Assignment of Names and Numbers (ICANN), or the licensing of companies in the business of creating processing power who would oversee the creation and distribution of credits. Users with vulnerabilities and no credits would have a specific time period to fix the exposure and would additionally have to make a payment to the entity that discovered the vulnerability. As a result, one could envision entrepreneurial users who are in the business of discovering vulnerabilities and profiting from these payments. By defining property rights, the full cost of these vulnerabilities would fall on the owners of the insecure machines.

Given this proposal, one must recognize that there are some potential information problems on the part of regulators, as discussed in Section 5, regarding the specifics of the permits. For instance, regulators will not know the right amount of vulnerability credits to assign in order to get the optimal level of vulnerability. Further, there is the potential for bureaucratic barriers to establishing and maintaining the credit system, especially if it is governed by a government agency. This may limit the effectiveness of this remedy.

Who's to Protect Cyberspace?

Another potential market solution is the continued growth of the already existing cyber insurance market. In addition to traditional insurance coverage, an increasing number of insurance companies are offering coverage for cyber breaches.[30] These insurance policies include coverage against damage related to hack attacks, viruses, network downtime, identity theft and the misuse of proprietary data and information. Cyber insurance is potentially beneficial on several fronts.

For one, there is an internal pressure on companies to maintain a level of security that minimizes their premiums. Insurance companies will develop standards that firms are required to meet. Given that this is a relatively new market, there is no reason to expect that it will not continue to grow as better actuarial data is collected and insurance companies gain a better understanding of how IT systems operate.

There is currently debate about what role the government should take in the cyber insurance market. Some argue that the market should be left to its own devices with market-determined premiums accurately reflecting the risks. Others argue that the government should guarantee cyber insurance and/or put a cap on the insurance policies.[31] Although we avoid engaging in an analysis of this issue, the economic principles discussed in previous sections, specifically issues of economic calculation, can add much insight into this debate regarding the ability of government to effectively regulate this market.

---

[30] The Insurance Information Institute estimates that cyber insurance could generate $2.5 billion in annual premiums by 2005. Source: Samuel Greengard, "The Real Cost of Cybersecurity," *Business Finance*, April 2003, pp. 52-55. Available at: http://www.businessfinancemag.com/magazine/archives/article.html?articleID=13957&pg=1 (last accessed 6/8/04)

[31] The Terrorism Risk Insurance Act, signed in November of 2002, created a three-year federal program that backs insurance companies in addition to guaranteeing that certain terrorist-related claims will be paid.

Who's to Protect Cyberspace?

Closely connected to the subject of cyber insurance, yet another potential means of internalizing externalities is extending liability to software authors and/or system operators. In the absence of being held liable, it is argued that these parties have a weak incentive to provide security because they do not incur the full costs of their failure to do so. Fisk (2002) concludes that it would be more effective to extend product liability to system operators as compared to software developers. One reason for this conclusion is that the existence and importance of open source software poses problems for making developers liable. Those that contribute open source software receive no income to offset potential liabilities. Purchasing cyber insurance would be one way of protecting against liability, but would also raise the cost of contributing open source code, so we would expect a decrease in the amount of open source software produced.

Fisk concludes that holding system owners liable is more reasonable and advocates an insurance system where liability for cyber accidents is "expected and accepted without stigma" (2002: 4). Similar to the automobile industry, system operators would be required to carry insurance against unexpected events. Fisk contends that the insurance industry would have similar beneficial effects on cyber security to those discussed above. He also envisions the creation of an Underwriters Laboratory that would certify software as secure and create an environment that encouraged effective cyber security.

We have not provided an exhaustive list of all possible courses of action. Instead, our aim here has been to highlight several potential courses of action for policymakers to consider. It is not our goal to endorse any one of these alternatives as being better than the others. Instead, our purpose is to emphasize that whatever course of action

policymakers choose, their focus should be on ensuring that the desirable aspects of the market are able to function effectively.

7. Conclusion

Without a doubt, the issue of cyber security will remain an important policy issue in the future. We have offered some insight into this issue from an economic perspective. In addition to the policy implications discussed above, we can put forth several general guiding principles:

1. Economics is a critical aspect of cyber security – Our main argument is that economics has been neglected in the policy debate regarding the most effective means of securing cyberspace. The basic concepts discussed in this paper can offer key insights into the best course of action. Admittedly, obtaining the necessary information to utilize these concepts will not always be easy. Nonetheless it is clear that neglecting the economic aspects of the issue will lead to incomplete and incorrect analyses.
2. National cyber security must be "demystified" – A key aspect of the cyber security issue is understanding the interconnectedness of the cyber environment. Given the interconnected nature of cyber space, the term "national security," in the context of cyber space, is simply the aggregate of individual Internet users whether for personal or business use. One must be careful not to think of "national security" as something that would fail to exist in the absence of government. As Schneier points out, we need to "demystify" Internet security (2003: 271). Security is all around us in our daily lives in a multitude of ways and

individuals take steps to secure their property, information and transactions. Cyber space is no different

3. Cyber security policy should rely on the market to the greatest extent possible – Economic analysis provides key insights into limitations in both the market and government settings. Given that the market provision of goods and services is preferable to government provision, from an economic standpoint, policy should aim to internalize externalities while maintaining the effectiveness of the profit/loss mechanism in efficiently allocating resources.

References

Anderson, Ross. 2001. Why Information Security is Hard: An Economic Perspective. Proceedings of the 17th Annual Computer Security Applications Conference, 358 – 365.

Anderson, Ross. 2002. Maybe we spend too much? Workshop of Economics and Information Security, University of California, Berkeley, May 16-17. http://www.cl.cam.ac.uk/users/rja14/econws/37.txt.

Buchanan, James M. 2003. Public Choice: The Origins and Development of a Research Program. Center for the Study of Public Choice, George Mason University, Fairfax, VA.

Camp, L. Jean, and Stephen Lewis, eds. 2004. *Economics of Information Security.* KluwerAcademic Publishers.

Camp, L. Jean, and Catherine Wolfram. 2000. Pricing Security. *Proceedings of the CERT Information Survivability Workshop*, Boston, MA, 31-39.

Cheswick, William R., and Steven M. Bellowing. 1994. *Firewalls and Internet Security: Repelling the Wily Hacker*. Reading, MA: Addison Wesley.

Computer Security Institute and Federal Bureau of Investigation. 2004. *CSI/FBI Computer Crime and Security Survey*. http://i.cmpnet.com/gocsi/db_area/pdfs/fbi/FBI2004.pdf.

Fisk, Mike. 2002. Causes & Remedies for Social Acceptance of Network Insecurity. Workshop of Economics and Information Security, University of California, Berkeley, May 16-17. http://www.cl.cam.ac.uk/users/rja14/econws/35.pdf.

Froomkin, Michael. 1997. The Internet as a Source of Regulatory Arbitrage. In *Borders in Cyberspace*, edited by Brian Kahin and Charles Nesson. Massachusetts: MIT Press, 129-163.

Gordon, Lawrence A., Martin P. Loeb, and William Lucyshyn. 2003. Sharing Information on computer systems security: An Economic Analysis. *Journal of Accounting and Public Policy* 22: 461-485.

Johnson, David R., and David G. Post. 1996a. And how shall the Net be governed? A meditation on the relative virtues of decentralized, emergent law. http://www.cli.org/emdraft.html.

Johnson, David R., and David G. Post. 1996b. Law and borders – the rise of law in cyberspace. *Stanford Law Review* 48: 1367-1405.

Lessig, Lawrence. 1999. *Code and other laws of cyberspace*. New York: Basic Books.

McMillan, John. 2002. *Reinventing the Bazaar*. New York: W.W. Norton and Company.

Mitnick, Kevin D., and William L. Simon. 2002. *The Art of Deception: Controlling the Human Element of Security.* Indiana: Wiley Publishing, Inc.

Mockus, Audris, Roy T. Fielding, and James Herbsleb. 2000. A Case Study of Open Source Software Development: The Apache Server. *Proceedings of the 22nd international conference on Software engineering (ICSE2000)*, 263-272.

Pollitt, Mark M. 1997. Cyberterrorism: Fact or Fancy? *Proceedings of the 20th National Information Systems Security Conference*. October: 285-89. http://www.cs.georgetown.edu/~denning/infosec/pollitt.html.

PricewaterhouseCoopers. 2000. *Security Benchmarking Service/InformationWeek's*

2000 Global Information Security Survey. Summary available at: http://www.pwcglobal.com/extweb/ncpressrelease.nsf/docid/7ABBA8E73B1E901D8525693500548A34.

Ranum, Marcus J. 2004. *The Myth of Homeland Security*. Indianapolis: Wiley Publishing. Inc.

Reidenberg, Joel R. 1996. Governing networks and cyberspace rule-making. *Emory Law Journal* 45: 911-926.

Schneier, Bruce. 2002. Computer Security: It's the Economics, Stupid. Workshop of Economics and Information Security, University of California, Berkeley, May 16 -17. http://www.cl.cam.ac.uk/users/rjal4/econws/18.doc.

Schneier, Bruce. 2003. *Beyond Fear: Thinking Sensibly About Security in an Uncertain World*. New York: Copernicus Books.

SecurityStats.com. 2004. *Virus Statistics*, January 16, 2004.http://www.securitystats.com.

Verton, Dan. 2003. *Black Ice: The Invisible Threat of Cyber-Terrorism*. New York: McGraw-Hill.