International Journal of the Commons
Vol. 7, no 1 February 2013, pp. 92–112
Publisher: Igitur publishing
URL:http://www.thecommonsjournal.org
URN:NBN:NL:UI:10-1-114407

ISSN: 1875-0281

Crowdsourcing cyber security: a property rights view of exclusion and theft on the information commons

Gary M. Shiffman
Center for Security Studies, School of Foreign Service, Georgetown University, Washington DC, USA
gms24@georgetown.edu

Ravi Gupta
Co-Founder and Chief Technology Officer, Alexandria, VA, USA
ravi@enkidu7.com

Abstract: Individuals increasingly rely upon the internet for basic economic interaction. Current cyber security mechanisms are unable to stop adversaries and hackers from gaining access to sensitive information stored on government, business, and public computers. Experts propose implementing attribution and audit frameworks in cyberspace to deter, prevent, and prosecute cyber criminals and attackers. However, this method faces significant policy and resource constraints. Social science research, specifically in law and economics, concerning common-pool resources suggests an organic approach to cyber security may yield an appropriate solution. This cyber commons method involves treating the internet as a commons and encouraging individuals and institutions to voluntarily implement innovative and adaptive monitoring mechanisms. Such mechanisms are already in use and in many cases have proven more effective than attribution mechanisms in resisting and tracing the source of cyber attacks.

Keywords: Commons; cyber security

Acknowledgements: We are grateful to Paul Rosenzweig, Elinor Ostrom, Gary Becker (DHS), Alex Kisselburg, Hugh Brooks, and several anonymous reviewers for their helpful comments. This study was funded, in part, by the US Department of Homeland Security (DHS) through the Center for Risk and Economic Analysis of Terrorism Events (CREATE) at the University of Southern California. However, any opinions, findings, conclusions, or recommendations are solely those of the authors and do not necessarily reflect the views of DHS or CREATE.

1. Introduction

Continued economic growth and development requires communication, and the internet significantly enhances global communications (Organization for Economic Co-Operation and Development 2008). Economic and other forms of security require security in the internet [The White House "Remarks by the President" (Their 2009)]. Numerous recent attacks highlight the security gaps prevalent in the country's cyber infrastructure [Lynn 2010; Symantec Corporation 2010; New York Times August 13, 2008 (Markoff 2008); Wall Street Journal December 17, 2009 (Gorman et al. 2009)]. For instance, computer viruses have stolen the credit card information of millions of American citizens, and they have accessed computers that control vital public infrastructure such as nuclear facilities [The White House "Cyberspace Policy Review" 2009; Christian Science Monitor September 21, 2010 (Clayton 2010)]. Due to increasing global threats, the U.S. government lists the protection of cyber space as one of the nation's most pressing national security priorities ("Cyberspace Policy Review"). Indeed, former Secretary of Homeland Security Michael Chertoff said: "Cybersecurity is among our first rank of security priorities in the twenty-first century" (Chertoff 2010, p. 1). Identity or assigning permanent identity markers to internet users based on their real-world identities, and audit or constantly collecting and sifting through massive amounts of data on internet use comprise the foremost ideas for providing security on the Internet. Even if wildly successful, an attribution framework where every internet user has a permanent identity and the state audits their internet use data will address only some cyber vulnerabilities. It will prove incapable of delivering sufficient cyber security to ensure economic and national security (Wheeler 2003; Hunker 2008; United States House Committee on Science and Technology 2010). Social science literature that relates to (1) the protection of commons resources such as fisheries and (2) the creation of economic growth and security in cities can inform our thinking on the internet as a commons. This article proposes that while identity and audit comprise essential elements of the traditional solutions to the "tragedy of the commons," the adoption of institutions with bottom-up, organic rules and voluntary governance regimes will offer additional necessary measures to secure the internet. Organic rules are bottom-up rules that naturally arise from the interactions between individuals as opposed to top-down rules that central authorities create and mandate.

2. Current cyber security method

Of the popular frameworks actively debated, solving "identity and audit" provides the most promise for security. Anonymity without forensics creates a corrupting dynamic in which actions are separated from consequences. If nobody knows who you are or what you do, you cannot get caught, prosecuted, and punished. Basic economic science tells us that when the cost of a good declines, the quantity demanded increases; conversely, when the cost increases, the quantity

demanded decreases. Knowing the identity and tracking the actions of individuals on the internet will allow for apprehension, prosecution, and the imposition of consequences (ibid). The cost of nefarious actions will increase, and their frequency of occurrence will decrease (Becker 1968).

The Obama administration advocates the implementation of parts of such an identity and audit framework. The policy dictates the establishment of authentication mechanisms that inform network authorities about the trustworthiness of internet users ("Cyberspace Policy Review," p. 33). To implement such an idea, the government will empower institutions with the ability to verify the identity of users. After verification by an authority, a user receives access to a protected network and its levels of data. Other users on the network will then know for certain that the individual accessing their service is indeed who they claim to be. If that person commits an illegal act, the network's authorities will immediately identify the culprit. Naturally the networks will exclude users who are unwilling to reveal their identity. Additionally, the government will assemble and survey vast amounts of internet usage data to find evidence of illegal activity. The government will then possess the forensic information required to find and prosecute the perpetrator (Hunker 2008; Shachtman 2010; United States House Committee). Note that the government has not yet indicated exactly how it would implement such an identity and audit framework, or provide institutions the ability to verify the identity of users.

The private sector provides good examples of where the government wants to go. The music industry association, the Recording Industry Association of American (RIAA) traces the IP address of users who illegally share copyrighted music to identify the perpetrator. Many music sharing software programs do not hide the IP address of the users, which makes it easy for the RIAA to find IP addresses. The RIAA then contacts the Internet Service Provider (ISP) that provided the IP address to the user, and asks them to turn over the identity of the user. However, the ISP may resist handing over the identity of the user and so the RIAA is not always successful Rampell (2008). As an additional example, Google discovered in early 2010 that hackers in China had attacked its websites. Following this discovery, Google partially terminated its services in China [New York Times, January 13, 2010 (Jacobs and Helft 2010)].

Although the existing informal attribution framework is successful at stopping some cyber crime, it cannot provide adequate cyber security for several reasons. First, cyber criminals and spies will increasingly mask their identity or exploit that of a third party. For example, attackers use "laundering hosts," by which an attacker logs into a random system and then uses or hijacks that system to attack his or her target. The hijacked system becomes an intermediary between the attacker and the target, obscuring the true source of the attack from authorities. The intermediary system can even belong to a verified user who is unaware of his or her computer's hijacking (Wheeler 2003, p. 3). Attackers also often launch attacks, such as denial of service attacks, from more than one physical location and in conjunction with numerous accomplices spread out over the globe. This tactic makes it difficult for

authorities to pinpoint the physical attacker to a single location (Hunker 2008, p. 7). Future plans for bolstering the attribution framework will make it more difficult for attackers to use these methods, but the history of cyber security and the literature on arms races suggest that hackers are adaptive and will draw the authorities into an expensive and never ending cat-and-mouse game [Gray 1971; Wheeler 2003, p. 46; Washington Post February 1, 2010 (Goldsmith 2010)].

Second, centralization increases vulnerability. Attackers will capitalize on the centralization inherent in the attribution model to perform increasingly devastating crimes. To verify the identity of users, a central authority must collect, analyze, and store information about those users. If a cyber criminal hacks into that central authority's network, in one fell swoop the criminal will gain access to sensitive information and the identities of millions of internet users (United States House Committee; Wheeler 2003, p. 48). As another example, if a cyber criminal successfully spoofs an identity, he or she could gain access to more: personal e-mail accounts, bank accounts, and health records.

Third, many oppose an identity and audit framework because they hesitate to sacrifice anonymity and privacy to gain security. They fear losing the advantages that a large, anonymous internet provides. The internet has arguably become a hub of creativity because it gives individuals the freedom to participate and contribute in a way they would feel uncomfortable doing if they lacked anonymity [Wheeler 2003, p. 50; Hunker 2008, p. 10; Forbes November 29 (Their 2012)]. The heated debates over legislative bills that the U.S. Congress has considered to patrol activity on the internet suggest that the government will likely face significant legal challenges trying to defend its ability to curtail and monitor activity that many people consider protected under the First Amendment of the U.S. constitution. Moreover, verified identification will produce an extension of property rights to the internet and give groups the ability to exclude and essentially discriminate against people who either are not verified or refuse to become verified. Implementation of property rights and exclusionary regimes will spawn a fragmentation of the internet into various closed private networks that will result in the diminished availability of information. Such an enclosure and resultant denial of access to knowledge occurred in the early 1990s when scholarly societies facilitated the privatization of scholarly journals and turned over their publishing apparatuses to private firms. To contain costs and increase profits, the private firms drastically increased the price of scholarly journals. Subsequently, many universities and libraries stopped purchasing subscriptions to the journals, causing many faculty and students to lose access to scholarly knowledge (Heller 1998; Kranich 2007). Additionally, the debate over net neutrality suggests that a significant population will resist further enclosure and the resultant privatization and commodification of information [Hahn and Wallsten 2006; Economides 2008; Wall Street Journal September 20, 2010 (Schatz 2010)].

Fourth, an identity and audit policy will require significant resource costs. The government and other participating institutions will require an enormous amount of resources to verify users and maintain the verification regime (Wheeler 2003,

p. 46). The U.S. government will also find it difficult to convince the nations from which many computer attacks arise, such as Southeast Asian and Eastern European countries, to participate (Kshetri 2005; Hunker 2008, p. 14). Additionally, it is unclear exactly how the government would implement a comprehensive identity and audit framework. The technical problems involved with implementing the framework may incur significant costs.

Fifth, an attribution framework will fail against computer viruses that rely on social networks and hardware to spread. These new strains of computer viruses propagate malware exponentially and nonlinearly throughout the internet, which makes it difficult if not impossible for authorities to uncover the origin of the attack and thereby deter cyber criminals. The Conficker virus, which resides in millions of government, home, and business computers in over 200 countries, is an example of such a malware. The virus, which consists of cutting-edge code, infected computers in a discreet fashion that circumvented the defenses of private business and government networks. Governments have yet to identify the creator of the virus. Furthermore, the fragmentation of the internet into private or semi-private enclaves will not have stopped the virus because it also traveled through hardware such as flash drives [Network World March 31, 2009 (McMillan 2009), July 31, 2009 (Greene 2009); Bowden 2010]. As discussed below, a voluntarily formed group of computer security experts made the greatest headway against Conficker – not a central authority relying on attribution and audit mechanisms. Groups of volunteers have also made contributions to cyber security that is not limited to the Conficker virus episode such as developing free threat detection software [Honeynet Project 2008, 2010; Washington Post March 30, 2009 (Krebs 2009)].

Identity and audit is the best of today's popular approaches to security on the internet. This policy, however, can never deliver the needed security and growth. It also generates conflict of interest for governments. Government agencies that have the task with providing cyber security also have the task of exploiting weaknesses in cyber security to collect intelligence. We must think outside of the existing framework for more transparent and accountable, and better solutions (Schneier 2009). Exploration of the parallels between commons, knowledge commons, and common pool resources will provide important foundational insights. Studies on enhancing and securing a commons support the idea that groups of individuals can voluntarily form to guard a common space. So how do we know if the internet is a commons?

3. The internet as a commons

A "commons" denotes resources that are shared between numerous participants. For example, a pasture is a commons, and the grass in the pasture "resource units." The participants are the farmers whose cows graze on the grass in the pasture. For decades, social scientists have applied this commons concept to resources such as forests, playgrounds, air, fisheries, and libraries (Hess and Ostrom 2007, 4–6).

Likewise, the internet is a shared resource. The information available on the public internet, made up of networked computers and servers, is the resource unit, and the participants involved comprise hundreds of millions of individuals and institutions around the world. Indeed, others have also considered the internet and cyber space as a commons (Hurwitz 2009; Rattray et al. 2010).

Despite the distinct similarities between a common-pool resource and the internet, the internet differs from a common-pool resource in three important ways. First, the resource units in the internet are non-rival. A common-pool resource, or shared resource system, contains a subtractable or rival resource. When a participant consumes a subtractable resource, the amount of the resource available to other participants decreases. When a farmer's cow eats the grass on an area of the pasture, the cows of other farmers can no longer eat that grass (Hess and Ostrom 2007, p. 9). In contrast, the internet, which is similar to other knowledge or information commons, does not house subtractable resources since information is typically non-rivalrous. When sharing a cooking recipe, knowledge spreads and does not diminish through sharing; when I give you Aunt Shirley's spaghetti sauce recipe, I still have the recipe. When a participant consumes or accesses information on the internet, that information is not deleted nor is it denied to other participants. In fact, the act of sharing a specific piece of information adds resource units to the commons and often adds value to that information (ibid., 7–11). Additionally, the redundancy of the information on the internet also reduces its subtractability. In theory, the elimination of a server or computer that hosts certain information may cause loss of that information and thus lead to a subtraction in resource units. However, in practice, individuals and organizations usually back up and cache information on several servers and computers, making it unlikely that elimination of a server or computer will lead to actual subtraction of information.

Second, as an information commons, the internet provides additional resource units as the number of participants increases. The non-rival resource units in an information commons allow users to accrue consistent benefits and encourage the users to maintain the commons. Contrary to a CPR, the more users in an information sharing commons, for example Wikipedia, the more valuable the commons (Alchian and Demsetz 1973; Hess and Ostrom 2007; Ostrom 2009).

Third, the internet is excludable. A commons can be privately, semi-privately, or collectively owned. Forms of private ownership allow the excludability of resource units. Participants may fence off sections of a commons and deny others access to that space and the resources contained within (Hess and Ostrom 2007, pp. 7–11). For example, farmers put up fences on areas of pasture to keep the cows of other farmers from entering and grazing on their land. The fenced land, however, ceases to be a part of a commons by nature of the fence (and associated property rights). It is no longer shared. Individuals can divide cyber space into various types of commons. The ease of erecting boundaries in the internet and the possibility of carving up smaller spaces allows internet users to partition the cyber commons into sub-commons and regulate the number of users (Alchian and Demsetz 1973;

Hess and Ostrom 2007; Ostrom 2009). For instance, many organizations own and operate private networks or private "clouds" that hold sensitive or proprietary information. These organizations verify the identity of individuals and only then provide them with access to the information and capabilities of their private network. These organizations create private commons that deny access or exclude internet users based upon identity. The private internet enclaves function as club goods (Buchanan 1965). For instance, the U.S. Department of Defense maintains classified information on private networks (Lynn). An individual gains access to one of these networks, for example, only after the network owner verifies identity and validates the individual's request to access that data. The user, in exchange, agrees to abide by certain constraints. In another method of internet exclusion, cyber attackers can use an attack called "denial of service" to deny their targets access to the internet entirely. These denial-of-service attacks overwhelm and effectively shut down a website's host server [Hunker 2008, p. 7; New York Times August 6, 2009 (Wortham 2009)].

Although parts of the internet function as club goods, much of the internet functions as a commons. You cannot separate the security of the private internet enclaves from that of the larger public internet commons. The private internet enclaves are often linked to each other and to the larger public internet, and so depend on the proper functioning of the larger internet commons. For example, one private internet service such as Amazon's cloud servers host the information of other private internet services. If Amazon's cloud servers suffer an attack and go down, other private internet services also go down. The attacks arise from individuals using the larger public internet to manufacture and deploy the attacks [Venture Beat May 4, 2011 (Takahashi 2011)]. Thus, the functioning and security of private internet enclaves is linked to the functioning and security of the larger public internet commons. Also, large parts of the internet are open to the public, and in fact this public internet provides the diversity, communication, and crowdsourcing that have proven so fundamental to the value of this knowledge commons and the generation of private enclaves of the internet (Becker and Ostrom 1995). As mentioned above, exclusion from the large commons – the public internet – diminishes both the private benefit and the public good. We see that institutions use cyber space by both benefiting from the unrestricted internet but also by creating enclaves with identity and audit regimes and constraints on behavior. Industry and government have evolved collaboratively in this direction (Homeland Security and Defense Business Council). However, using the commons framework allows us to characterize cyber security threats in two ways: penetration of your enclave, and denial of your access to the value of the broader internet value. Thus, we see that the internet is a unique commons that has both low subtractability and high excludability. Despite a few key differences, the internet still shares many similarities with other common-pool resources. Therefore, reviewing how security provision best functions for other common-pool resources can help us articulate how security provision should function for the internet.

4. Bottom-up, organic security

A rich social science literature establishes that the participants of a common-pool resource can organize organically to protect and even enhance resource units. The traditional economic allegory states that in conditions without regulation, the self-interested participants negligently over-consume the resource and destroy the commons. This idea is known as the *tragedy of the commons* (Hardin 1968). For instance, each farmer receives the full benefit of adding an additional cow to the commons pasture, but only pays a fraction of the common resource costs. Therefore, each farmer will over-invest in cattle and undervalue the grazing land. The accumulated grazing of the total cows eventually results in the depletion of the grass – the common pool resource. Social scientists led by recent Nobel Laureate Elinor Ostrom suggest two ways to solve this "tragedy of the commons."

Property rights based upon centralized enforcement and property division comprise the standard approaches to solving the "tragedy of the commons." One either invokes a strong central authority to regulate the behavior of participants or divides the commons up into parcels owned by individuals, thereby dividing the common property into private property via cordons or fences, or some combination of both. The autocratic form of ownership incentivizes rules and enforcement consistent with commons resource preservation – the autocrat benefits from long-term preservation. The owner or central authority establishes rules and implements enforcement mechanisms, and monitors the behavior of participants, denying access or excluding participants who do not follow the rules (ibid; Alchian and Demsetz 1973, 16–27). When divided into parcels with fences, the individual owners of the small plots of land ensure others do not encroach on their property, protecting their valuable resource units. The allegorical solution to the commons tragedy mirrors today's popular approaches to cyber security – strong centralized authority, mostly across private or semi-private enclaves.

The common property rights-based solution framework fails to secure and enhance the commons. Several elements mitigate the effectiveness of the top-down or "fences" approaches. First, a disassociated regulator may not have the details or adaptive capabilities to effectively allocate resources of the commons and may make the "tragedy" worse. Second, the privatization of a commons often diminishes the value of the commons. Several studies point out these consequences. A 2006 article showed that centrally regulated and cordoned-off forest areas in Brazil were more vulnerable to fire and deforestation than indigenous reserves that used a bottom-up approach, discussed below (Nepstad et al. 2006). Additionally, an investigation of more than 200 protected areas in twenty-seven countries found that many protected areas, regulated via a top-down approach that excluded much of the public, did not have adequate control over their boundaries (World Wide Fund 2004). Third, numerous studies revealed that a commons is better taken care of when a population local to the commons or the commons' participants play a role in monitoring the health of the commons regardless of the type of ownership

or regulatory regime. The lack of exclusion provides for a greater number of people monitoring the health of the resource (Banana and Gombya-Ssembajjwe 2000; Ostrom and Nagendra 2006).

According to the alternate framework for regulating a common-pool resource, participants organically establish rules via a bottom-up or collective approach that regulates resource consumption (Ostrom and Nagendra 2006, p. 19224). Currently, numerous commons not regulated via a top-down approach function well. Such commons include California groundwater basins, North Atlantic fisheries, African community forests, and Nepalese irrigation systems (Hess and Ostrom 2007, p. 11). A survey of forests and parks in South Asia found that buffer-zone forests, which are not centrally-protected or regulated, and community-managed forests often experience significantly more regrowth than government-controlled forests (Nagendra et al. 2005). In other words, collectively-managed or public common-pool resources are often more sustainable than centrally-regulated or privatized commons.

Apart from the examples above, laboratory studies also demonstrate that humans come together as a group voluntarily to regulate each other's behavior, promote the group, and ultimately their individual interests (Olson 1993; Van Vugt 2009). One such study asked students to invest a specific amount of tokens in two types of markets. The experimenters fixed the return for the first market for every token the students invested while they pegged the return for the second market to a function where the return would increase depending on how many tokens all the students in the group invested. If all the students invested their tokens in the first market, each would receive a return of $1.25 per round, whereas if all participants put all of their tokens in the second market, each would receive the maximum return of $1.89 per round. When the students made their investment decisions without interacting with the other students, they each averaged a return of 21% of the maximum attainable return. After ten rounds, the students engaged in face-to-face communication with each other for ten minutes. The students reportedly did not discuss coordinating their investment behavior and instead engaged in "cheap talk." After this brief communication period and another ten rounds, the students averaged a return of 55% of the maximum. The students next talked to each other face-to-face between each of the next ten rounds. The students then averaged a return of 73% of the maximum (Ostrom and Nagendra 2006, p. 19229). When the students interacted with each other, they realized the benefits of coordinating their behavior and working together as a group. Other variations of this study revealed that humans are also willing to forgo immediate individual return in order to sanction and reward the behavior of others. This regulatory behavior allows groups to better coordinate their behavior and eventually increase their individual returns (Sefton et al. 2006). If we think of the internet as a commons, and we know empirically and experientially that people can protect a commons and organize in the absence of centralized rule making and enforcement, then the commons framework provides a relevant approach to security in cyber space.

5. Security without identity

Individuals also organize in an organic way to protect against external threats in the absence of identity. For example, Jane Jacobs identified this behavior in relation to the way in which cities and neighborhoods function. In *The Death and Life of Great American Cities,* Jacobs described a block in a diverse, urban city as a commons open to the public and largely autonomous. She then discussed how the interactions of the residents and visitors of the city block led those individuals to form an informal but effective policing apparatus that established security. According to Jacobs, when humans are free to routinely interact with others, they tend to develop informal networks of relationships based upon trust and open access to news and information. An open and diverse city block allows pedestrians, salesmen, and residents, who may not know each other's identity, to interact and develop these relationships that lead to spontaneous actions of policing (Jacobs 1961). In this instance, the block provides a common space with countless resource units, all requiring physical security. People gain little from a common space with run-down and dangerous areas and so will invest little to nothing to protect the space and the strangers inhabiting it.

Jacobs illuminates the idea that knowledge without identity leads to collective security through a personal anecdote when she describes a scene that she witnessed from her apartment window, which was located in a teeming city block. A small girl was standing rigidly on the street, facing a man who was cajoling her to follow him. The girl looked uncomfortable and hesitant, which the owners of the butcher shop across the street noticed. As the man became more demanding, the owners walked out in the street with crossed arms and a stern look. Eventually, other shopkeepers and customers walked out and residents began to poke their heads out from the apartment buildings on top of the shops. This newly formed group surrounded the man and the girl. The man noticed the group and changed his behavior toward the girl. Even though no one knew the girl or the man, the group made it clear to the man that they would protect the girl. The group soon learned that the man was the girl's father and of no threat to the girl (ibid). From their front steps, the residents of Jacob's city blocks provided security to an individual without knowing her identity or that of her possible assailant. To do so, all they required was the ability to witness the suspect behavior. At the same time, we've also read the news stories of the victims being beaten on the street with pedestrians in earshot, but nobody responds to help the victim. In these instances, we usually understand the common space to have little value to those individuals in relation to the costs of organic security.

6. Organic security on the internet

The internet is a commons that is conducive to organic security and security without identity. Individuals voluntarily join together to defend a common resource without a strong autocratic authority or identity. Rules and enforcement occur organically, but some conditions are more conducive, such as the size of the

commons, the value of the common resource to participants, and the number of participants. Referring again to Ostrom, Social Science research provides factors that help us understand preservation and security of a commons (see Figure 1).

Figure 1 presents ten factors that Ostrom identified as integral to the health of a collectively-controlled commons. It displays the impact of each factor on common-pool resources and the ways in which the factors can be applied to the internet commons. The table therefore gives us a framework for analyzing the internet in order to identify factors more and less conducive to security and the cyber commons. In the next section, we will examine the Conficker virus attack to see how individual users of the overarching internet commons will voluntarily come together to monitor potential cyber attacks and defend against them. We choose the Conficker virus episode because it is well documented and shows the comparison between organic versus top-down cyber security. We will show that identity and audit is not encompassing, and that a commons framework can fit the internet and lead to growth and security without an autocracy over identity.

7. The Conficker virus case

The Conficker virus episode illuminates how the bottom-up approach can outperform the top-down approach. As mentioned above, the Conficker computer virus spread rapidly. It infected and ultimately gained control of millions of computers around the world, some of which provide access to vital infrastructure. Cyber security experts first detected the virus in November 2008 when they noticed its existence in computers designed to attract viruses and cyber attacks known as "honeypots." The virus exploited a vulnerability in the Microsoft Windows operating system, which allowed the virus to spread to other computers easily and rapidly. The virus replicated and installed itself in computers so quickly that it dislodged competing viruses. Soon after experts discovered the virus's existence, they realized it had already spread to hundreds of thousands of computers around the world. Experts also soon came to understand that authorities had failed to notice the virus for so long because the virus was intelligent enough not only to disable anti-malware programs but also fix the vulnerability it had exploited and essentially erase any trace of infection [Bowden; Washington Post March 30, 2009 (Krebs 2009); Network World March 31, 2009 (McMillan 2009), July 31, 2009 (Greene 2009); United Press International March 25, 2009; New York Times March, 18 2009 (Markoff 2009)].

Eventually, Microsoft released a security patch to fix the vulnerability, but that did not end the virus's spread. Some users failed to download and install the new patch, which made it easy for the virus to spread as it did originally. At the same time via the internet, the virus received updates to its code that gave it the ability to profligate over flash drives. Curiously, the virus did not appear to affect the performance of the computer in any way. All it did, other than spread, was occasionally send a few hundred bytes over the internet to a seemingly random assortment of domain names. Like a sleeper cell biding its time before it attacks its host, the virus essentially lay in wait in the computer, subtly communicating

Factor	Impact on the commons	Impact on the internet
Size of the commons	If the size is large then the cost of defining boundaries is high. If small, then the system does not generate enough benefit. Thus a moderate sized system is the most conducive to ensuring success.	People split the larger public internet commons into private, semi-private, and public enclaves that then fall under the purview of various organizations, so the size of the commons can vary. Smaller commons limit resource availability.
Productivity of the commons	If resources are depleted or overly abundant then participants do not face incentives to conserve.	Not only is the internet non-subtractive – as a knowledge commons, it produces more benefits from more participants.
Predictability of commons dynamics	Participants must estimate the consequence of their actions.	The internet provides robust reliability in the absence of denial of service or identity threats. As information on the internet proliferates, knowledge becomes a function of tools or widgets on the internet that allow for search and other functions.
Resource unit mobility	Since organizing is costly, it is less likely to happen when the resource is mobile and can dissipate such as water that can evaporate.	Since information is not subtractable, the information does not move to some other location, unless cordoned off into an enclave – a private cloud.
Number of participants	The number of participants must not be too low or too high so as to overwhelm the resource system.	The internet commons successfully sustains hundreds of millions of internet participants. Organization occurs among sub-populations.
Leadership	Experts and elites with entrepreneurial skills help organize and lead participants.	The internet provides perhaps the most entrepreneurial space in the history of the world.
Norms/Social capital	Users with agreed upon rules of behavior, norms of reciprocity, and sufficient trust between each other adhere to agreements and perform sufficient surveillance.	The success of e commerce sites such as e-bay and Craig's list validate the importance of social norms and reputation effects.
Knowledge of the system	Participants are more successful maintain the commons when they understand the system and the consequences of their actions	A large group of experts exists, however most users do not understand the operation of the internet. Participants, however, have clear expectations of the benefits and costs of the system and the consequences of their actions.
Importance of resource to participants	Participants should place a high value on the resource.	The global economy, public infrastructure, and military capabilities are highly dependent on the internet.
		However of interest, most people may not fully appreciate how reliant they are on the effective functioning of the internet.
Collective-choice rules	A commons is more successful when participants have full autonomy at the community level to craft and enforce their rules.	The openness of the internet provides great autonomy, however the anonymity can make coordination more difficult. Social media and networking may enhance communication and therefore community level-rulemaking and enforcement.

Columns "Factors" and "Impact on the Commons" from: Ostrom, A General Framework for Analyzing Sustainability of Social-Ecological Systems 2009. Column "Impact on the Internet" added here.

Figure 1: Factors that determine the health of a collectively-controlled commons.

with its remote command center and listening for the signal to launch its strike with only its creator aware of the destruction it will bring (ibid).

No one could stop the virus's spread or identify its creator until a number of computer security experts voluntarily worked together to battle the virus. Since the virus had been spreading in all directions throughout the internet, no one could ascertain exactly which computer it infected first and thus trace its source of origin. To solve this problem, a unique and small group of cyber security experts from various nonprofit foundations and technology companies voluntarily came together and formed a group known initially as the Conficker Cabal and today as the Conficker Working Group ("CWG"). The CWG members represent such groups as America Online, Symantec, Georgia Institute of Technology, Shadowserver Foundation, Internet Coporation for Assigned Names and Numbers, and China's Ministry of Information Industry. Microsoft offered a reward of $250,000 to encourage this group and others to hunt down the person behind the virus. The CWG members did not sign contracts, ask for fees, or set up official meetings and workshops. They only use a website, email mailing lists, and occasional conference calls to coordinate their work. The CWG tried to follow the path of the information the virus was sending back to its command center. However, the path the information took was complex and difficult to decipher. One of the CWG members then visited online forums that catered to hackers and cyber security aficionados. On the forum, the CWG member picked up a few snippets and rumors that suggested the creator of the Conficker virus was situated in Ukraine. Also, on this forum, many computer security experts not affiliated with the CWG also gave the CWG member advice on how to battle the virus. Over time, the CWG members and their affiliated organizations developed software to detect the presence of the virus on computers and networks and eliminate it. The Department of Homeland Security has since distributed this software to federal and local governments, commercial vendors, and infrastructure owners. The creator or creators of the virus are still at large. However, Mikko Hypponen, chief research officer at F-Secure and a member of the CWG, disclosed that government authorities are close to identifying and capturing the responsible party. Hypponen indicated that the authorities believe the creators are in Ukraine (ibid; Conficker Working Group, "Confiker Working Group", 2010).

The events surrounding the spread of and response to the Conficker virus impart several lessons. First, the hacker who created and launched the virus capitalized on the enormous number of participants on the internet and the ubiquity of computer and social networking to rapidly and secretly spread the virus in all directions, thereby making it nearly impossible discover its origin. Second, as mentioned before, the virus's ability to spread discreetly through the internet and via hardware erased the security that private networks typically provide. Third, volunteers who were not associated with the proper authorities were the most successful in combating the virus. Like when the shopkeepers and residents of Jacob's neighborhood spontaneously protected the girl against an unknown attacker, a small group of experts from around the world saw the threat, and chose to come together with the help of some major organizations and voluntarily

organized into a cyber enforcement squad. Many members of the CWG believe that government law enforcement agencies were slow to respond to the virus [New York Times March 18, 2009 (Markoff 2009)]. Experts from various organizations can organically organize and respond to future cyber attacks.

8. Steps to strengthen collective cyber security

A central authority such as the U.S. government can undertake several steps to encourage the organization of security collectives such as the Conficker Working Group and improve their shortcomings. The Conficker Working Group published a lessons learned document that highlighted several deficiencies including the need to improve communication and coordination (Conficker Working Group, "Lessons Learned Document" 2010). Security researchers and experts can, and in many cases do, communicate with each other and self-organize. However, we should not take their ability to do so for granted. In a normal commons such as a fishery, the close physical proximity of the participants involved helps them build relationships and thus improve coordination and security. In a limited physical space, individuals run into each other regularly and are compelled to interact. In cyber space, interactions are less happenstance and meaningful relationships are more difficult to construct. Central authorities must help promote interaction and provide the space where security experts and others can build trust relationships that foster coordination and communication. Organizations such as Oracle and Apache provide similar spaces and undertake similar steps to aid the development of open-source software (Apache; Oracle).

Social science literature provides numerous insights on the importance of interaction and how authorities must structure virtual spaces to aid coordination and communication. Research has shown that the willingness of individuals to work as a group is positively correlated with their ability to identify with the group, trust each other, and satisfy their core values (Baumeister and Leary 1995; Ostrom 2003; Van Vugt 2009). As mentioned above, human interaction increases the likelihood that people will work together. A study found that verbal messages exchanged in chat rooms increases subjects' propensity to contribute to a public good nearly as much as face-to-face communication (Bochet et al. 2006). Communications tools that improve the ability of internet users to interact with each other can increase coordination and improve security. Furthermore, studies showed that individuals are more likely to act ethically or pro-socially when they feel someone is evaluating them and when their actions impact their reputations (Bateson et al. 2006). Sites such as eBay allow users to comment on the reputations of others, which impacts economic behavior (Resnick and Zeckhauser 2002; Ostrom 2003). Major websites can also implement reputation mechanisms, such as eBay's feedback systems, that deter users from pursuing unlawful or ethically questionable behavior. Also, studies found that individuals are motivated to act in a certain way when they receive incentives to do so, either for material gain or the fulfillment of a core value (Van Vugt 2009). The government and relevant organizations can somehow, even if

through recognition, reward the efforts of professional and amateur security experts in responding to cyber crime. The government and major technology companies can help certain populations such as military entities and nongovernmental organizations use attribution technology to build smaller, semi-private networks that have a core group of verified individuals yet do not completely restrict access. Cyber security experts will then find it easier to coordinate their actions and monitor their part of cyber space. When an illegal activity occurs in semi-private enclaves, experts can use an audit mechanism to identify the individual, collect information from individuals monitoring the cyber space, and trace back the source of the illegal activity. Although a central authority cannot guarantee cyber security on its own, it can use the commons framework and crowdsourcing to guide actions that will facilitate a security with high visibility and low identity that relies on semiautonomous groups to counter unpredictable cyber threats (Vermeij 2008).

Utilizing crowdsourcing on the internet to combat threats is not new to the U.S. government. The Department of Homeland Security recently established the "Neighborhood Network Watch" program to analyze potential terrorist usage of American internet networks. The program aims to educate Americans about cyber security, collect samples of data over public networks to identify malicious behavior, and incentivize individuals and organizations to report suspicious cyber behavior that relates to terrorism.

The Neighborhood Network Watch program's focus on educating internet users about cyber security signifies the small steps each individual can take to help secure the internet. Other organizations such as information technology security company Symantec and the Federal Trade Commission also incentivize internet users to become responsible cyber citizens and secure their personal information and consequently help care for the internet. These organizations urge internet users to, for example, regularly update anti-virus programs, use firewalls, identify phishing scams, properly dispose computers, and password protect home networks. They communicate to individuals that by following such steps, individuals will better protect their personal information and reduce the likelihood of suffering identity theft. This incentivizes and thus encourages participation. Greater participation improves the overall security of personal information and home networks on the internet and helps curtail the spread of malware and thwart cyber criminals. The steps taken by individual actors helps to ensure the security of personal information, but significantly helps to curtail the spread of malware on the internet (United States Government 2011).

The specific ways in which the U.S. government can leverage the expertise of participants in the internet commons differs according to the type of cyber attack. Cyber threats differ in scale and intensity. Criminals and spies more frequently launch denial-of-service, hacking, and probing attacks against a small number of websites and cause little damage to national security systems. A nation-state, however, has the ability to organize a catastrophic cyber assault against another nation's security system even though such attacks occur infrequently. With respect to frequent and less damaging attacks, the U.S. government can allow

computer security experts from relevant organizations to take the lead. These experts have more local information and can quickly implement solutions at the target site. On the other hand, with respect to less frequent and more damaging attacks, a U.S. government agency can take the lead in battling the assault. In such a scenario, local actors and experts can still provide the lead government agency with information and expertise. Thus, during a potential cyber war with a nation such as China, the U.S. government can coordinate and scale-up the efforts of numerous experts and solution implementers (IBM 2010).

The U.S. government can encourage collective cyber security irrespective of the nationality of the local actors and experts. The internet does not subscribe to geographical boundaries. For instance, when Russia allegedly launched the world's first cyber war against Estonia in 2007, Estonian government authorities fought the assault with computer experts not only from Estonian government, police, banks, and internet service providers but also experts from Finland, Germany, and Slovenia [New York Times May 29, 2007 (Landler and Markoff 2007)]. Experts from non-Western countries also have an incentive to organize and protect the internet. Many countries use the internet for commerce, safety, and public services (Deibert and Rohozinski 2010). During the Conficker virus episode, representatives from the Chinese government worked with Americans and Europeans to protect the internet's underlying vitality and their computers' functionality. The U.S. government can further encourage international participation in collective cyber security by highlighting the economic and social incentives international actors have in defeating cyber threats and protecting access to the internet.

Multinational private organizations have similar incentives to help secure the internet. Some of the most lucrative companies in the world such as Google and Apple depend on the internet to reach customers and sell products. Such economic incentives are seemingly increased when the vulnerabilities of a company's product give rise to or help propagate the threat. In mid-2010, the Stuxnet virus attacked infrastructure-monitoring computer systems built by Siemens. The virus gained control of key computer systems in Iran's nuclear facilities and wreaked havoc [Christian Science Monitor September 21, 2010 (Clayton 2010); The Guardian September 26, 2010 (Beaumont 2010)]. The virus then spread to similar computer systems in other countries. Within weeks, Siemens, working alongside Symantec and others, released a detection and removal tool for the virus to ensure the security and viability of their product (Siemens; Murchu 2010). Lastly, major technology companies such as Google and Facebook have considerable in-house cyber security and technology expertise that the U.S. government can leverage to help collectively police the internet by encouraging them to share best practices and pool resources when required.

9. Conclusion

The Conficker Working Group represents self organization, organic rules, and improved audit in the absence of autocratic identity and audit regimes. Like the

city shop keepers and neighbors, when people have an interest in the abiding value of a commons and associated resource units, they will face incentives necessary to enhance and secure the commons. The role of government in these instances, properly conceived, entails harnessing the power of the individual participants, organically, or crowdsourcing. Social science work – theory, field work, and experimentation – provides these insights:

- Any measure that keeps consequences tied to personal actions remains critically important regardless of type of authority, ownership, or identity regime. For example, when costs, privacy, or other hurdles prevent the verification of identity, like on a busy city street, good visibility remains important.
- Communication among commons participants, even without full identity, leads to enhanced outcomes for the commons. In conditions where the size of the population, or nature of relationships, facilitates trust and reciprocity, security and growth will be enhanced.

We understand that identity and audit regimes, even when implemented perfectly, will fail to prevent sufficient solutions to provide security. Therefore, as we consider cyber space and policies to secure economic and national security interests, policymakers must keep in mind the lessons from the commons. We propose that policymakers and cyber security professionals bolster existing identity and audit security with organic, crowdsourced approaches typically found in other commons.

Literature cited

Alchian, A. and H. Demsetz. 1973. The Property Right Paradigm. *Journal of Economic History* 33(March 1973):16–27.

Apache. *Welcome to the Apache Software Foundation*, http://www.apache.org.

Banana, A. and W. Gombya-Ssembajjwe. 2000. Successful Forest Management: The Importance of Security of Tenure and Rule Enforcement in Ugandan Forests. In *People and Forests: Communities, Institutions, and Governance*, eds. C. Gibson, M. McKean, and E. Ostrom, MIT Press, Cambridge, MA: 87–98.

Bateson, M., D. Nettle, and G. Roberts. 2006. Cues of Being Watched Enhance Cooperation in a Real-World Setting. *Biology Letters* 2(3):412–414.

Baumeister, R. F. and M. R. Leary. 1995. The Need to Belong: Desire for Interpersonal Attachments as a Fundamental Human Motivation. *Psychological Bulletin* 117:495.

Beaumont, P. 2010. Iran Nuclear Experts Race to Stop Spread of Stuxnet Computer Worm. *The Guardian.* September 26, 2010. http://www.guardian.co.uk/world/2010/sep/26/iran-stuxnet-worm-nuclear.

Becker, G. 1968. Crime and Punishment: An Economic Approach. *Journal of Political Economy* 76(2):169–217.

Becker, C. D. and E. Ostrom. 1995. Human Ecology and Resource Sustainability: The Importance of Institutional Diversity. *Annual Review of Ecology and Systematics* 26:113–116.

Bochet, O., T. Page, and L. Putterman. 2006. Communication and Punishment in Voluntary Contribution Experiments. *Journal of Economic Behavior and Organization* 60:11–26.

Bowden, M. 2010. The Enemy Within. *The Atlantic Magazine,* June 2010 http://www.theatlantic.com/magazine/archive/2010/06/the-enemy-within/8098/.

Buchanan, J. 1965. An Economic Theory of Clubs. *Economica* 32:1–14.

Chertoff, M. 2010. Foreward. *Journal of National Security Law and Politics* 4(1):1–6.

Clayton, M. 2010. Stuxnet Malware is 'Weapon' Out to Destroy...Iran's Bushehr Nuclear Plant? *Christian Science Monitor.* September 2010. http://www.csmonitor.com/USA/2010/0921/Stuxnet-malware-is-weapon-out-to-destroy-Iran-s-Bushehr-nuclear-plant.

Conficker Working Group. 2010. *Conficker Working Group.* http://www.confickerworkinggroup.org/wiki/pmwiki.php.

Conficker Working Group. 2010. *Conficker Working Group Lessons Learned Document*, June 17. http://www.confickerworkinggroup.org/wiki/uploads/Conficker_Working_Group_Lessons_Learned_17_June_2010_final.pdf.

Deibert, R. and R. Rohozinski. 2010. Risking Security: Policies and Paradoxes of Cyberspace Security. *International Political Sociology* 4(1):15–32.

Economides, N. 2008. "Net Neutraliy", Non-Discrimination and Digital Distribution of Content Throughout the Internet. *Journal of Law and Policy for the Information Society* 4:209–233.

Goldsmith, J. 2010. Can We Stop the Global Cyber Arms Race? *Washington Post.* February 1, 2010. http://www.washingtonpost.com/wp-dyn/content/article/2010/01/31/AR2010013101834.html.

Gorman, S., Y. Dreazen, and A. Cole. 2009. Insurgents Hack U.S. Drones. *Wall Street Journal* December 17, 2009: A1.

Gray, C. 1971. The Arms Rache Phenomenon. *World Politics* 24(39):39–79.

Greene, T. 2009. Conficker Talk Sanitized at Black Hat to Protect Investigation. *Network World.* July 31, 2009. http://www.networkworld.com/news/2009/073109-black-hat-conficker-talk.html.

Hahn, R. and S. Wallsten. 2006. The Economics of Net Neutrality. *The Economists Voice Article* 3(6):1–7.

Hardin, G. 1968. The Tragedy of the Commons. *Science* 162:1243.

Hayes, T. and E. Ostrom. 2005. Conserving the World's Forests: Are Protected Areas the Only Way. *Indiana Law Review* 38:595–617.

Heller, M. 1998. The Tragedy of the Anticommons. *Harvard Law Review* 111(621):621–688.

Hess, C. and E. Ostrom. 2007. Introduction: An Overview of the Knowldge Commons. In *Understanding Knowledge as a Commons*, eds. C. Hess and E. Ostrom, 4–6. MIT Press, Cambridge, MA.

Homeland Security and Defense Business Council. 2010. The 9/10/11 Project: Cyber Security. http://homelandcouncil.org/pdfs/pdfs/hsdbc_cyber_security_91011_projectmonograph.pdf.

Honeynet Project. 2008. *Developments of the HoneyD Virtual Honeypots.* http://www.honeyd.org/.

Honeynet Project. 2010. *About the Honeynet Project 2010.* http://www.honeynet.org/about.

Hunker, J. 2008. Role and Challenges for Sufficient Cyber-Attack Attribution. Institute for Information Infrastructure Protection, January 2008.

Hurwitz, R. The Prospects for Regulating Cyberspace: A Schematic Analysis on the Basis of Elinor Ostrom, General Framework for Analyzing Sustainability of Social Ecological Systems, Science, vol. 325 (July 24, 2009), 419 – 422, 2009, http://web.mit.edu/ecir/pdf/hurwitz-ostrom.pdf

IBM. 2010. Meeting the Cybersecurity Challenge: Empowering Stakeholders and Ensuring Coordination. White Paper, February 2010.

Jacobs, J. 1961. *The Death and Life of Great American Cities.* New York: Random House.

Jacobs, A. and M. Helft. 2010. Google, Citing Attack, Threatens to Exit China. *New York Times*, January 13, 2010: A1.

Kranich, N. 2007. Countering Enclosure: Reclaiming the Knowledge Commons. In *Understanding Knowledge as a Commons*, eds. C. Hess and E. Ostrom. MIT Press.

Krebs, B. 2009. Flaw in Conficker Worm May Aid Cleanup Efforts. *Washington Post.* March 30, 2009. http://voices.washingtonpost.com/securityfix/2009/03/flaw_in_conficker_worm_may_aid.html.

Kshetri, N. 2005. Pattern of Global War and Crime: A Conceptual Framework. *Journal of International Management* 11:541.

Landler, M. and J. Markoff. 2007. Digital Fears Emerge After Data Siege in Estonia. *New York Times,* May 29, 2007. http://www.nytimes.com/2007/05/29/technology/29estonia.html.

Lynn, W. 2010. Defending A New Domain: The Pentagon's Cyberstrategy. *Foreign Affairs*, October 2010.

Markoff, J. 2008. Before the Gunfire, Cyberattacks. *New York Times*, August 13, 2008: A1.

Markoff, J. 2009. Computer Experts Unite to Hunt Worm. *New York Times*, March 18, 2009: A17.

McMillan, R. 2009. Group takes Conficker Fight to a New Level. *Network World.* March 31, 2009. http://www.networkworld.com/news/2009/040109-group-takes-conficker-fight-to.html.

Murchu, L. O. 2010. *Stuxnet P2P Component.* http://www.symantec.com/connect/blogs/stuxnet-p2p-component.

Nagendra, H., M. Karmacharya, and B. Karna. 2005. Evaluating Forest Management in Nepal: Views Across Space and Time. *Ecology and Society* 10(24):1–16.

Nepstad, D., S. Schwartzman, B. Bamberger, M. Santilli, D. Ray, P. Schlesinger, P. Lefebvre, A. Alencar, E. Prinz, G. Fisk, and A. Rolla. 2006. Inhibition of Amazon Deforestation and Fire by Parks and Indigenous Lands. *Conservation Biology* 20(1):65–73.

Olson, M. 1993. Dictatorship, Democracy and Development. *American Political Science Review* 87(3):567–576.

Oracle. *Oracle and Java*, http://www.oracle.com/us/technologies/java/overview/index.html.

Organization for Economic Co-Operation and Development. 2008. *The Future of the Internet Economy*. http://www.oecd.org/sti/interneteconomy/40780975.pdf. June 2008

Ostrom, E. 2003. Towards a Behavioral Theory Linking Trust, Reciprocity and Reputation. In *Trust and Reciprocity: Interdisciplinary Lessons from Experimental Research*, eds. E. Ostrom and J. Walker. Russell Sage, New York, NY.

Ostrom, E. 2009. A General Framework for Analyzing Sustainability of Social-Ecological Systems. *Science* 325(July 2009):419–422.

Ostrom, E. and H. Nagendra. 2006. Insights on Linking Forests, Trees and People from the Air, on the Ground and in the Laboratory. *PNAS*, December 2006: 19224–19231.

Rampell, C. 2008. How It Does It: The RIAA Explains How it Catches Alleged Music Pirates. *The Chronicle of Higher Education.* May 13, 2008. http://chronicle.com/article/How-It-Does-It-The-RIAA-Ex/786/.

Rattray, G., C. Evans, and J. Healey, American Security in the Cyber Commons" In *Contested Commons: The Future of American Power in a Multipolar World*, Edited by A.M.Denmark and J. Mulvenon. Washington, DC: Center for a New American Security, 2010, http://www.cnas.org/files/documents/publications/CNAS%20Contested%20Commons_1.pdf

Resnick, P. and R. Zeckhauser. 2002. Trust Among Strangers in Internet Transcations: Empirical Analysis of eBay's Reputation System, Vol. 11. In *The Economics of the Internet and e-Commerce (Advances in Applied Microeconomics)*, eds. M. Baye and J. Maxwell. Emerald Group, Bingley, UK.

Schatz, A. 2010. Net Neutrality Activists Target Google as Talks Heat Up. *Wall Street Journal.* September 20, 2010. http://blogs.wsj.com/digits/2010/09/20/net-neutrality-activists-target-google-as-talks-heat-up/.

Schneier, B. 2009. *Who Should Be in Charge of Cybersecurity?* http://www.schneier.com/essay-265.html.

Sefton, M., R. Shupp and J. Walker. 2006. The Effect of Rewards and Sanctions in Provision of Public Goods. *CAEPR Working Paper.* August 29, 2006. http://papers.ssrn.com/sol3/papers.cfm?abstract_id=932683.

Shachtman, N. 2010. Spooks in the Machine: How the Pentagon Should Fight Cyber Spies. *Progressive Policy Institute.* http://www.progressivefix.com/wp-content/uploads/2010/01/Spooks-in-the-Machine_Jan2010.pdf.

Siemens. April 2011. *Information Concerning Malware/Virus/Trojan.* http://support.automation.siemens.com/WW/llisapi.dll?func=cslib.csinfo&objid=43

876783&nodeid0=10805583&caller=view&lang=en&siteid=cseus&aktprim=0&objaction=csopen&extranet=standard&viewreg=WW.

Symantec Corporation. 2010. 2010 Cybercrime Report: United States. http://www.symantec.com/content/en/us/home_homeoffice/media/pdf/cybercrime_report/Norton_USA-Human%20Impact-A4_Aug4-2.pdf.

Takahashi, D. 2011. Amazon cloud server was used to attack Sony, *VentureBeat*, May 14, 2011, http://venturebeat.com/2011/05/14/amazon-cloud-server-was-used-to-attack-sony/.

The White House. 2009. Cyberspace Policy Review. http://www.whitehouse.gov/assets/documents/Cyberspace_Policy_Review_final.pdf.

Their, D. 2009. Remarks by the President on Securing Our Nation's Cyber Infrastructure. May 29, 2009. http://www.whitehouse.gov/the-press-office/remarks-president-securing-our-nations-cyber-infrastructure.

Their, D. 2012. The Return of SOPA? Controversial Bill Sponsor Lamar Smith to Chair House Tech Committee, *Forbes*, November 29, 2012, http://www.forbes.com/sites/davidthier/2012/11/29/the-return-of-sopa-controversial-bill-sponsor-lamar-smith-to-chair-house-comittee-on-science-space-and-technology/.

United Press International. 2009. Conficker Cabal Goes After Computer Worm. March 25, 2009. http://www.upi.com/Top_News/2009/03/25/Conficker-Cabal-goes-after-computer-worm/UPI-14801237929348/.

United States Department of Defense. "Quadrennial Defense Review." 2010. http://www.defense.gov/qdr/images/QDR_as_of_12Feb10_1000.pdf.

United States Department of Homeland Security. 2008. *Neighborhood Network Watch.* March 18, 2008. http://www.dhsnnw.org/.

United States Government. 2011. *OnGuard Online*. http://www.onguardonline.gov/.

United States House Committee on Science and Technology. July 2010. Planning for the Future of Cyber Attack Attribution. http://science.house.gov/sites/republicans.science.house.gov/files/documents/hearings/071510_Giorgio.pdf

Van Vugt, M. 2009. Averting the Tragedy of the Commons: Using Social Psychological Science to Protect the Environment. *Current Directions in Psychological Science* 18(2009):169.

Vermeij, G. 2008. Unpredictability and Evolution: Policy and the History of Life. In *Natural Security: A Darwinian Approach to a Dangerous World*, eds. R. Sagarin and T. Taylor. Berkeley: University of California Press.

Wheeler, D. 2003. Techniques for Cyber Attack Attribution. *Institute for Defense Analysis.* October 2003. http://www.dtic.mil/cgi-bin/GetTRDoc?AD=ADA468859&Location=U2&doc=GetTRDoc.pdf.

World Wide Fund for Nature. June 2004. Are Protected Areas Working? An Analysis of Forest Protected Areas. assets.panda.org/downloads/areprotectedareasworking.pdf

Wortham, J. 2009. Online Attack Silences Twitter for Much of Day. *New York Times*, August 6, 2009: B7.