2013 5th International Conference on Cyber Conflict
K. Podins, J. Stinissen, M. Maybaum (Eds.)

Legal Aspects of a Cyber Immune System

Janine S. Hiller
Department of Finance
Pamplin College of Business
Virginia Tech
E-mail: jhiller@vt.edu

Abstract: The malicious and criminal attacks against individuals, businesses, and nations on the Internet and in cyberspace must be mitigated in order to protect citizens and nations. One cyber security vision is the cyber immune system. Such a system would include automatic defense mechanisms based on incomplete attribution, continuous monitoring, pattern recognition, and the application of a set of rules designed to isolate or destroy the abnormal actor, or attacker. The cyber immune system would operate at a distributed level, at the speed necessary to thwart constant and ever changing threats. From a legal perspective, it matters if a state or private entity applies the system. For example, if a state actor is involved, then due process, and the protection of fundamental rights such as privacy and speech, are relevant to the action taken, while if a private entity applies the cyber defense then relevant legal issues include property, contract, and regulatory limits. While the automated nature of a cyber defense may present legal challenges to both state and non-state actors, it may mitigate the legal ramifications of human decision making if the system of rules is carefully crafted.

Keywords: *cybersecurity, privacy, property, speech, law*

1. INTRODUCTION

Concerted cyber attacks against the US banking system[1] are but one of the newest reported instances, among many, of the continuing and evolving threats against cyber entities. It is clear that "normal" cyber security is failing to mitigate threats and that new ideas for protecting citizens and nations should be considered. Technical security advances offer potential solutions for cyber defense, however they face legal uncertainties within a complex environment.

The original designers of the Internet focused on a free and open communications system, not foreseeing perhaps that the distributed design of the communications network would lead to its own insecurity.[2] But the values inherent in the design are those that imbue the medium with its power and ability to serve democratic principles. Novel applications of cyber security systems should incorporate society's values for privacy, freedom, and the rule of law into the distributed defense design. This task is made difficult because of the unique intersection of law and technology among different layers of state and non-state actors. Realizing that systems and actors will differ, this paper identifies, at a high level, the major legal issues that may arise in designing and implementing a cyber defense that is analogous to a human immune system composed of differing autonomous, distributed, learning systems that defend the person from attack. A holistic view of cyber defense is presented, emphasizing the potential contributions of a preventative, private law perspective. Because in many nations the cyber infrastructure is owned primarily by the private sector, actions that strengthen the cyber safety of those entities will ultimately strengthen national security. In addition, managing cyber security in the private sector will lead to fewer conflicts at the international level.

The type of technical system envisioned would include automatic defense mechanisms based on incomplete attribution, continuous monitoring, pattern recognition, and application of a set of rules designed to isolate or disable the abnormal actor, or attacker. Such a system would operate at a distributed level, at the speed necessary to thwart continuous and ever changing threats. The system would also be embodied systemically and limited to mitigative and preemptive actions, as opposed to individual, retributive action. From a legal perspective the

---

1 *See* Nicole Perlroth & Quentin Hardy, "Bank Hacking Was the Work of Iranians, Official Say," *New York Times* (January 8, 2012) *available* at http://www.nytimes.com/2013/01/09/technology/online-banking-attacks-were-work-of-iran-us-officials-say.html.

2 Chris C. Demchak, *Resilience and Cyberspace: Recognizing the Challenges of a Global Socio-Cyber Infrastructure (GSCI),* 14 J. Comp. Pol'y Analysis 254, 258-61 (2012) ("Cyberspace began as a pure document sharing mechanism for which security was about physical reliability, not human predatory behaviors.").

structure of the system is relevant and it matters if a nation-state or private entity applies the system. For example, if a state actor is involved, then due process, the protection of fundamental rights such as privacy and speech, are relevant to the action taken, while if a private entity applies the cyber defense then relevant legal issues include property, contract, and regulatory limits. While the automated nature of a cyber defense may present legal challenges to both state and non-state actors, it could possibly mitigate the legal ramifications of human decision making if the system of rules is carefully crafted.

2. IMMUNE TYPE DEFENSES

The goal of this section is to identify fundamental elements of an immune inspired cyber defense system that may invoke legal questions, thus facilitating discussion of the corresponding challenges of implementation in a democratic society. It is recognized that the technical level of discussion is general in nature and that the term cyber immune system, as described in this paper, could also incorporate common elements of certain artificial intelligence or intelligent systems.

Research in the 1990's described the metaphorical use of the human immune system to construct elements of a cyber security system.[3] These cyber defense elements seek to mimic the automatic actions of human cells and organs to respond to new, previously unknown threats, take defensive action, and internalize learning for future defense. Biancaniello et al. state that, "Artificial Immune Systems have enjoyed a number of application successes in Cyber Defense including web-server behavioral anomaly detection, network intrusion detection, the detection of malicious code execution, and operating system call monitoring."[4]

The US document, "Enabling Distributed Security in Cyberspace," describes current security as depending on reactive actions and human intervention.[5] Yet the Slammer worm infected 90 percent of its hosts in 10 minutes, scanning 55 million targets each second.[6] In order to defend against rapidly spreading, sophisticated, and persistent threats, the document identifies an Automated Course of Action (ACOA) as the first building block needed for a "Healthy Cyber Ecosystem."[7] The

---

[3] *See* Anil Somayaji et al., *Principles of a Computer Immune System,* 1997 New Security Paradigms Workshop 75 (1997).

[4] Paul Biancaniello et al., *AIR: A Framework For Adaptive Immune Response for Cyber Defense*, *available at* www.atl.lmco.com/papers/2021.pdf *at 3 (December 19, 2011), (an unclassified document prepared by authors from Delaware State University).*

[5] U.S. Dept. of Homeland Security, Enabling Distributed Security in Cyberspace 6 (2011).

[6] Id. at 6-7.

[7] Id. at 8-11.

human immune system is then used as a metaphor to describe the elements of such a system. The human system description includes multiple levels of defense, at both the cell and system level, including synchronization/communication, identification methods, and actions to destroy and/or immobilize an attack (for example, a virus). An automated cyber security system is conceptualized in a similarly decentralized and highly synchronized manner. Such a system could incorporate continuous monitoring, pattern recognition, and anomaly detection to identify non-entity threats, respond according to preset policies to block, shut down, or disable the threat, and then audit and share information among a system of users; all done automatically and at the speed of real time computer execution. The aggregation and maintenance of data is important within such a system so that adaptive/intelligent learning occurs. The ecosystem might include a centralized public entity that would facilitate sharing, learning, and techniques for immunization from future damage.

Within this broad description of a cyber immune system, certain data collection elements are required for effective implementation; IP and addressing information, deep packet inspection, data mining, and data retention. Like a human system that achieves immunities by "remembering" and defending against a virus, a fully operational cyber security/defense system will require longitudinal information about malicious actors and actions and continuous monitoring for both known and new threats. In addition, one must note that just like a human system, a cyber immune system will not operate perfectly; attribution may be based on probabilities, behavioral information, and past actions.

It is important to note that the *systematic* defense/security envisioned here is distinct from an individual "strikeback" offensive action.[8] Because these are individual retributive actions against particular perpetrators, they would not fall under an immune defense system that is adopted broadly in a community of users (the system) and operates to prevent damage and mitigate attacks. A private strikeback is legally suspect, although there have been arguments for supporting such action.[9] International law of warfare would apply to a nation taking such action, and would include such issues as attribution and self defense.[10] Adoption of an immune defense could potentially avoid the escalation of cyber conflicts by securing systems from attacks and vulnerabilities.

---

[8] For an exhaustive treatment of the law of cyber counterstrikes and a proposed way forward, see Jay P. Kesan & Carol M. Hayes, *Mitigative Counterstriking: Self-Defense and Deterrence in Cyberspace*, 25 Harv. J. L. & Tech. 415 (2012). Discussions indicate that industry offensive action is actually not a new phenomenon, although news reports are that it could be growing. *See* Dennis Fisher, Debate Over Active Defense and Hacking Back Crops up at RSA, Feb. 28, 2012, *available at* .http://threatpost.com/en_us/blogs/debate-over-active-defense-and-hacking-back-crops-rsa-022812 .

[9] *See Mitigative Counterstriking, supra* note 8, at 531-32.

[10] *See* Matthew E. Castel, *International and Canadian Law Rules Applicable to Cyber Attacks by State and Non-State Actors,* 10 Can. J.L. & Tech 89, 95-102 (2012). For a discussion of how the law of war would apply, see David E. Graham, *Cyber Threats and the Law of War,* 4 J. Nat'l Security L. & Pol'y 87 (2010).

Several examples can be used to illustrate components of an existing automated immune system, including continuous monitoring, data analysis, and automated action. The U.S. employs multiple information collection and monitoring methods within its National Cybersecurity Protection System, described as "an integrated system for intrusion detection, analysis, intrusion prevention, and information sharing"[11] in order to defend federal civilian systems. Different elements of the system collect network information, analyze the information to detect cyber threats, and distribute cyber security information across participating federal systems.[12] NCPS includes not only analysis and detection, but also intrusion prevention by agreement with Internet Service Providers that can take action against Internet traffic at the border of federal systems, i.e. as it enters or leaves those networks.[13] However, although some information sharing occurs voluntarily and will be expanded under the recent Executive Order,[14] the information collection system and defensive actions are limited to the federal civilian government and are not universally distributed.

In the private sector, Facebook describes its cyber system for security as "the Facebook Immune System because it learns, adapts, and protects in much the same way as a biological immune system."[15] Within their proprietary, closed platform, Facebook monitors users and their accounts in order to prevent criminal actions like stolen credit cards and passwords that can lead to economic losses. The automated system will not only halt the attack, it will take steps to destroy the "assets" of the attacker in order to dissuade future attacks. In 2011, Facebook utilized 2,000 servers, 200 models, and 20 billion daily checks to operate the system.[16] Being a social media company, Facebook faces unique risks; however, this example illustrates that a private entity will tailor its cyber security to meet the specific needs of its business, suppliers, and customers. It might be seen as a cyber immune system within that closed system, but does not reach the distributed and broader cyber immune model.

---

[11] U.S. Dept. of Homeland Security, Privacy impact Assessment for the National Cybersecurity Protection System (NCPS) 1 (July 30, 2012).

[12] Id. at 8-9 (includes EINSTEIN 1, 2, and 3, Security Information and Event Management (SIEM), Packet Capture (PCAP) as well as other technical elements).

[13] Id. at 18.

[14] Executive Order, "Improving Critical Infrastructure Cybersecurity" (Feb. 12, 2013), *available at* http://www.whitehouse.gov/the-press-office/2013/02/12/executive-order-improving-critical-infrastructure-cybersecurity.

[15] "National Cybersecurity Awareness Month Recap and the Facebook Immune System," November 10, 2011, http://www.facebook.com/notes/facebook-security/national-cybersecurity-awareness-month-recap-and-the-facebook-immune-system/10150352042420766 .

[16] Id. *See also* Tao Stein et al. "Facebook Immune System," *available at* http://research.microsoft.com/en-us/projects/ldg/sns2011prog.aspx.

Japan has reportedly contracted with Fujitsu to develop a protective virus that will detect, trace, and disable malware or attackers across networks.[17] The unique aspect of the proposed virus is that it would act automatically to follow the attack back across multiple computers, collect information, and take action to neutralize the attack at each stage. Many details are unknown about the Japanese system, but its highly automated and distributed actions seem to meet some of the elements of an immune system.

It is also worth noting future potential developments of programs that can be likened to an immune system. In September, 2012, the U.S. Department of Homeland Security and the Department of Commerce issued a Request for Information entitled; "Developing a Capability Framework for a Healthy and Resilient Cyber Ecosystem Using Automated Collective Action."[18] The RFI sought information about the feasibility and challenges of pursuing a system that would include "automated information sharing and collective action, reference data, machine learning, behavior monitoring based on business rules, interoperable systems and organizational policies, and authenticated users and systems."[19] Reports linked existing programs in the Energy Department and the Federal Aviation Administration to this concept of a "learning, self-healing network."[20] Utilizing the concepts described in the NCPS, and intrusion protection platforms, a future system would, at least theoretically, provide for real-time automated responses to cyber intrusions across a wide infrastructure.

Interestingly, in February, 2013 a paper written by the New England Complex Systems Institute in 2008 for the Chief of Naval Operations Strategic Studies Group was released; it was titled, "Principles of Security: Human, Cyber and Biological."[21] The authors described the human immune system and its ability to evolve defenses. The report noted, by comparison, the inherent security weakness of the Internet architecture that transports communication packets in content neutral fashion. In conclusion the authors suggested two alternatives; distributed automatic security at

---

[17] Yomiuri Shimbun, "Govt working on defensive cyberweapon/Virus can trace, disable sources of cyber-attacks," *Daily Yomiuri Online* (January 3, 2012) *available at* http://www.yomiuri.co.jp/dy/national/T120102002799.htm.

[18] U.S. DEPT. HOMELAND SECURITY, DEVELOPING A CAPABILITY FRAMEWORK FOR A HEALTHY AND RESILIENT CYBER ECOSYSTEM USING AUTOMATED COLLECTIVE ACTION (Request for Information) (2012).

[19] Id. at 3.

[20] William Jackson, "Agency programs show outlines of future cyber ecosystem," *Government Computer News* (November 9, 2012) *available at* http://gcn.com/Articles/2012/11/09/Agency-programs-show-outlines-of-future-cyber-ecosystem.aspx. *See also* Peter M. Fonash, "Identifying Cyber Ecosystem Security Capabilities," Sept./Oct. 2012 Crosstalk 15 (2012) (cross referencing types of attacks with desired cyber ecosystem/defense design).

[21] Blake Stacey & Yaneer Bar-Yam, New England Complex Systems Institute, Principles of Security: Human, Cyber and Biological (2008).

the user level or a change in Internet protocols so that routers could inspect content for malware.[22]

In summary, currently there are partial automated cyber immune defense systems at some stage, public and private, but no complete system exists. Visions for a system include systems monitoring, longitudinal information collection, deep packet inspection, information sharing, system "learning," and proactive, automated action to takedown or quarantine bad actors based on behavioral and technical information. If a cyber immune system were to be employed at a national level, private sector actors as well as network administrators would be essential participants. In contrast to a military operation that depends on a hierarchy of command and control, a cyber immune system is distributed among all participants in order to exponentially increase the security of the network. Vast amounts of information about port scans, attack methods, signatures, behavioral actions, and the like is shared so that the immune system can learn about vulnerabilities and block attacks or cure weaknesses in defense, and redistribute the aggregated knowledge for individual action.

While many technical issues remain in the adoption of a metaphorical cyber immune ecosystem, they are matched by the legal and policy questions engendered as well.

3. LEGAL ISSUES

A system such as the cyber immune defense system described is never simply a technical solution to a thorny problem; it is "political to its very core,"[23] as the design and implementation will embody societal values and choices in a democratic society.[24] Data collection that aggregates great volumes of content related information longitudinally can identify patterns of harmful activity, yet can also threaten individual privacy and chill speech. Information sharing can provide the needed tools to prevent damage to systems and property, yet has the potential to thwart checks on government involvement in citizens' lives. The automated takedown or quarantine of websites, domain names, or software is necessary to respond in real-time to prevent illegal activity and maintain national security, yet its imperfect application can impede speech rights, violate property, and potentially undermine democratic discourse. The following discussion highlights these fundamental legal issues.

---

[22] Id. at 10-12.

[23] Helen Nissenbaum, *Where Computer Security Meets National Security*, 7 Ethics & Info. Tech. 61, 62 (2005).

[24] Id.

Legal protection of electronic property is built in part on criminal laws, including the Computer Fraud and Abuse Act (CFAA)[25] in the United States, and domestic laws that enforce the international Budapest (Cybercrime) Convention.[26] The CFAA makes unauthorized access of protected computers (including those connected to the Internet, by interpretation) a crime; intentional unauthorized access to federal computers does not require damage, while intentional or reckless access to other computers can require that damage occur, such as the loss of intellectual property or the degradation of the system.[27] The international Cybercrime Convention and the European Union Framework Decision on attacks against information systems[28] provide similar prohibitions against illegal access to information systems, illegal system interference, and illegal data interference.[29]

A cyber immune defense imagines a distributed approach that goes beyond the traditional deterrence effect of criminal actions, therefore requiring a broader analysis of actions by not only the government, but also the private sector. Application of the system should take into account the ways that the design of the technology implicates the important areas of speech, privacy, and property. The following sections discuss these areas and the basic laws that apply based on whether the action is led by government or the private sector.

A. *SPEECH*

Government Action. Freedom of speech is enshrined in fundamental laws across the globe, and the First Amendment in the US prevents the government from limiting free speech; even computer code has been interpreted to be a form of speech.[30] The recent Middle East changes provide a reminder of how important free speech is to political discourse; a discourse that occurred significantly due to Internet communications. Although protection of speech may vary in application between leading democracies,[31] it is undeniable that the right of speech is essential to the preservation of fundamental freedoms.

---

[25] Counterfeit Access Device and Computer Fraud and Abuse Act of 1984, 18 U.S.C. § 1030 (1984).

[26] Convention on Cybercrime, *opened for signature* Nov. 23, 2001, E.T.S. No. 185, *available at* http://conventions.coe.int/Treaty/en/Treaties/Html/185.htm.

[27] *See* Chris Kim et al., *Computer Crimes,* 49 Am. Crim. L.Rev. 443, 460-62 (2012).

[28] Council Framework Decision 2005/222/JHA of 24 February 2005 on attacks against information systems, *available at* http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:32005F0222:EN:NOT

[29] *See* Liis Vihul et al., Legal Implications of Countering Botnets 9 (2012).

[30] *See, e.g.,* Universal City Studios, Inc. v. Corley, 273 F.3d 429 (2d Cir. 2001).

[31] For example, the US and German conceptions of freedom of the press and speech differ. *See,* Christopher Witteman, *Information Freedom, a Constitutional Value for the 21st Century,* 36 Hastings Int'l & Comp. L. Rev. 145 (2013) (speech protected from a broader principle in Germany).

In order to identify malicious actions through behavioral information, signatures, and the like, a cyber immune system would automatically collect information and data from users' traffic longitudinally, thereby posing a real potential harm to the essential values of privacy and speech. The widespread collection of information about individual communications is extraordinarily sensitive, especially when an immune system would go further than collecting address and IP information, and would undertake deep packet inspection in order to detect and take action to neutralize malicious activity.[32] This type of packet inspection, reportedly used by China to block the websites it censors,[33] poses a great threat to individual liberties. Government application of these technologies to civilian networks is particularly problematic from the US standpoint; the current administration firmly opposed legislation, ultimately defeated, that would have allowed government agencies to monitor domestic private communications in order to actively defend them from attack.[34]

The rights to private life and freedom of expression and opinion are also protected in the Universal Declaration of Human Rights and in the treaty, the International Covenant on Civil and Political Rights.[35] In addition, in 2011 the UN Special Rapporteur for freedom of expression released a report that discussed the importance of Internet communications,[36] and ensuing coverage labeled the report as a declaration that Internet access is a human right.[37] Statutes in Estonia, Finland, France, and Costa Rica for example, provide a right to Internet access for citizens.[38] Any automated system will need to incorporate strong protections for protecting access in order to ensure rights to free speech.

---

[32] *See* Ted Stevenson, "Network Security Essentials: Deep Packet Inspection," Feb. 28, 2012, *available at* http://www.enterprisenetworkingplanet.com/netsecur/network-security-essentials-deep-packet-inspection.html (deep packet inspection is necessary to stop sophisticated attacks).

[33] Alex Wang, "What is Deep Packet Inspection?' Feb. 1, 2012 *available at* http://www.pcworld.com/article/249137/what_is_deep_packet_inspection_.html.

[34] Ellen Nakashima, *When is a cyberattack a matter of defense?* Wash. Post, Feb. 27, 2012 *available at* http://www.washingtonpost.com/blogs/checkpoint-washington/post/active-defense-at-center-of-debate-on-cyberattacks/2012/02/27/gIQACFoKeR_blog.html. The issue of monitoring foreign communications is a separate issue, and not discussed in this article.

[35] Kent Roach, *Must We Trade Rights for Security? The Choice Between Smart, Harsh, or Proportionate Security Strategies in Canada and Britain,* 27 Cardozo L. Rev. 2151, 2152-53 (2006) (speech rights may also be restricted when balanced with other interests under the doctrine of proportionality).

[36] Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, *Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, delivered to General Assembly*, U.N. Doc. A/HRC/17/27 (May 16, 2011).

[37] Nicholas Jackson, *United Nations Declares Internet Access a Basic Human Right*, The Atlantic, June 3, 2011, *available at http://www.theatlantic.com/technology/archive/2011/06/united-nations-declares-internet-access-a-basic-human-right/239911. See also* Young Joon Lim & Sarah E. Sexton, *Internet as a Human Right: A Practical Legal Framework to Address the Uniqure Nature of the Medium and to Promote Development,* 7 Wash. J.L. Tech. & Arts 295, 297 (2012).

[38] Victoria Ekstedt, Tom Parkhouse & Dave Clemente, *Commitments, Mechanisms & Governance, in* National Cyber Security Framework Manual 163-66 (Alexander Klimburg, ed., 2012).

Private Action. Actions by private parties that affect speech may not be prohibited in the same manner as those by government entities. Businesses control the use of their systems, and to meet the goal of maintaining network quality ISPs often have the right to manage and protect network traffic. United States law, for example, allows providers to monitor and even disclose communications in order to maintain service levels.[39] Agreements, formalized in contracts between service providers and their customers, delineate these management rights. Furthermore, general terms of use between private entities and the broader community of users can negotiate use limitations and access rights. The recent voluntary Copyright Alert System agreement between ISPs and copyright owners, whereby ISPs will monitor and notify users of potential copyright violations, is an example of a kind of mediation activity by ISPs.[40]

B. PRIVACY

Government. In the electronic world, speech and privacy are intertwined, as surveillance of communications can breach privacy of information and chill speech. The legality and extent of surveillance by governments varies greatly. A survey of law enforcement access to data in ten countries showed that in the midst of an investigation that in all ten countries access to electronic data was allowed; eight did not require approval of a formal request.[41] In comparison, the Fourth Amendment of the US Constitution prohibits unreasonable searches and seizures and requires probable cause for a warrant to obtain access to places when there is a reasonable expectation of privacy.[42] Thus, the law restricts government access to the content of electronic communications with judicial approval, but is not interpreted to restrict access to address information such as header or IP information. The Electronic Communications Privacy Act (ECPA), Stored Communications Act (SCA), and Wiretap Acts as well as other state and federal laws, protect the rights of citizens to privacy and autonomy.[43]

The ECPA, amended by the SCA, protects the privacy of electronic communications

---

[39] *See* Scott J. Glick, *Virtual Checkpoints and Cyber-Terry Stops: Digital Scans To Protect the Nation's Critical Infrastructure and Key Resources*, 6 J. Nat'l Sec. L. & Pol'y 1, 8 (2012).

[40] *See*, Peter Groh, *Through a Router Darkly: How New American Copyright Enforcement Initiatives May Hinder Economic Development, Net Neutrality and Creativity,* 13 U. Pitt. J. Tech. L. & Poly 1 (2012).

[41] *See* Steven C. Bennett et al., *Storm Clouds Gathering for Cross-Border Discovery and Data Privacy: Cloud Computing Meets the U.S.A. PATRIOT Act,* 13 Sedona Conf. J. 235, 247 (2012).

[42] *See Virtual Checkpoints, supra* note 39, at 9-12

[43] For a detailed discussion of how a myriad US laws meet the requirements of Section 15 of the Cybercrime Convention to safeguard human rights, for example, see Discussion Paper, Data Protection and Cybercrime Division, Directorate General of Human Rights and Rule of Law, *Article 5 Conditions and Safeguards under the Budapest Convention on Cybercrime,* Nov. 8, 2011, *available at* www.coe.int.

and applies to both the government and service providers. Police must seek a warrant to obtain communications in some cases, or a subpoena under other circumstances. Both criminal and civil penalties for violations are possible. However, exceptions allow entities to share information related to the investigation of computer trespass, and ISPs are allowed to share information in emergency situations.[44]

The Cybercrime Convention requires that competent authorities have access to specific data held by a person or system in whatever method it is stored, including traffic data. An ISP may be required to assist collecting and accessing the data. The convention anticipates that the request will be pursuant to an active investigation of wrongdoing, however.[45]

Private Action. As described above, the ECPA is the primary US law protecting privacy of electronic communications, and it prevents access by private parties, with some exceptions. One of the exceptions is based on consent of the party. For example, Google has reportedly shared information with government agencies in order to trace the source of a series of cyber attacks; arguably terms of use agreed to by customers allow Google to share personal information for the purpose of 'protecting the rights or property of Google or our users."[46]

In the EU, the Data Protection Directive, and other telecommunications acts,[47] apply to the private sector and ISP actions, and protect personally identifiable data. Through harmonized national laws, data collection requires user consent, is limited to the intended purposes, and individuals have the right to information about the data that is held about them. Differences in national laws occur, such as whether IP addresses are protected personal information.[48] An ISP involved in collecting personally identifiable information for a cyber immune system will invoke the provisions of the Directive unless consent is obtained.

C. PROPERTY

One of the major purposes of a cyber immune system is to protect the property of citizens and government from attack, therefore supporting the goal of national security. Property, though, can exist in multiple forms. Intellectual property, such

---

[44] *See* Gregory T. Nojeim, *Cybersecurity and Freedom on the Internet,* 4 J. Nat'l Security L & Pol'y 119, 125-28 (2010).

[45] *Cybercrime Convention, supra* note 26, at arts. 16-21.

[46] Stephanie A. Devos, *The Google-NSA Alliance: Developing Cybersecurity Policy at Internet Speed,"* 21 Fordham Intell. Prop. Media & Ent. L.J. 173, 209-212 (2010).

[47] *See* Vihul, *supra* note 29, at 49-53 (also comparing the national laws applied to ISPs in Estonia and Germany).

[48] Id. at 19 (national laws may differ in application however).

as trade secrets, business plans and the like, supports the economic stability of both business and the country, while the property of privately held critical infrastructures can consist of electronic controls that affect physical performance, such as the electric grid. Computer systems themselves are a form of property in which the right to exclude others is incorporated. The computers, controls and most of the ISP's[49] and networks that make up the Internet are primarily privately owned. In the United States, "virtually all broadband networks"[50] fall into the private ownership category, therefore implicating laws of private property. Ironically, the same laws that criminalize cyber attacks may also limit proactive cyber defense.

Government. Government action related to the rights of speech and privacy can also affect property in the electronic environment. The requirement of due process and fundamental fairness in areas of property and liberty could apply to an automated action taken in a cyber immune system; if the government takes down a website or restricts Internet access, principles of notice and an opportunity to be heard become relevant.[51] If malicious cyber actors use "innocent" computers to launch an attack and an automatic defense is triggered, innocent parties may be negatively affected by government action. In addition, if the implementation of an automatic cyber immune defense occurs across networks it could violate property rights in privately owned computers if it involves unauthorized access to private parties' proprietary system, or if it is beyond the authorization of a network provider, even though it intends to disarm a criminal actor.[52]

Private Action. Common law concepts of trespass to property can be applied to computer intrusions in addition to the cause of action for unauthorized access. An automatic system that accessed a website in violation of its terms of use has been held in the US to give rise to a claim of trespass;[53] without owner consent, such as an automatic virus update, a cyber immune system implemented by a private entity such as an ISP could run the risk of violating property rights. The argument has been made, however, that self-defense could allow mitigation across network property

---

[49] ISP and network operator are used interchangeably to designate an entry point to the network. While the paper does not discuss the potential involvement of Tier One telecommunications companies, the backbone operators, those companies may have some of the same opportunities for monitoring. (There are however, more difficult questions for monitoring at this level.) *See* James Andrew Lewis, Speech at the Sasakawa Peace Foundation: Rethinking Cybersecurity-A Comprehensive Approach (Sept. 12, 2011), *available at* http://csis.org/publication/rethinking-cybersecurity-comprehensive-approach.

[50] Charles B. Goldfarb & Lennard G. Kruger, Cong. Research Service, 7-7500, Infrastructure Programs: What's Different About Broadband? 2 (2009).

[51] *See* Daniel J. Steinbock, *Data Matching, Data Mining, and Due Process,* 40 Ga. L. Rev. 1 (2005). *Also see* Sean M. Condron, *Getting It Right: Protecting American Critical Infrastructure,* 20 Harv. J.L. & Tech. 403, 416-18 (2007) (noting due process importance, but also suggesting a balance).

[52] *See* James P. Farwell, *Industry's Vital Role in National Cyber Security,* 2012 Strategic Stud. Q. 10, 30 (2012).

[53] eBay v. Bidders Edge, 100 F. Supp. 2d 1058 (N.D. Cal. 2000).

lines.[54] In the EU, the 2009 Telecom Directive[55] requires public communication providers to 1) provide secure services, 2) report breaches, and 3) share a summary of material breaches with the European Network and Information Security Agency (ENISA).

4. DISCUSSION OF CYBER IMMUNE DEFENSE WITHIN THE GLOBAL SOCIO-CYBER CONTEXT[56]

Envisioning and implementing an automated cyber immune defense should intentionally preserve the fundamental rights that the security ultimately seeks to protect; property, privacy of communication, and speech. Legal limitations to protect these rights differ based on who will undertake the defensive steps, whether it be maintenance of a database to identify malicious actors or installation of software to purge victims' infected computers, for example.

Distributed security will require the participation of both private and state actors, both for effectiveness and for policy reasons.[57] ISPs may be particularly situated to play a role in the security ecosystem. Logs at the infrastructure level showed recently that 162 of 168 Fortune 500 companies were compromised by hackers at some point of time,[58] and an ISP has "unparalleled visibility into global networks"[59] being "well positioned to aid" in "proactive" actions.[60] An ISP is located within network infrastructure between victim and attacker, perhaps a kind of neutral zone, handling traffic that is not within the "perimeter" of either side. Automated actions taken to disable or immobilize an attack or bad actor could be designed as part of network management, analogous to how actions to stop spam have been taken in

---

[54] Kesan, *supra* note 8, at 520-21.

[55] EU Directive 2009/140/EC

[56] The term Global Socio-Cyber is found in Demchak, *supra* note 2 (Resilience and Cyberspace: Recognizing the Challenges of a Global Socio-Cyber Infrastructure).

[57] *See* Paul Rosenzweig & James X. Dempsey, *Einstein 3.0, in* Patriots Debate 115-34 (Harvey Rishikof, Stewart Baker & Bernard Horowitz, eds., 2012).

[58] Joseph Menn, *Hacked companies fight back with controversial steps*, *Reuters*, June 18, 2012 (Neustar found evidence of a breach at some point of time at companies).

[59] William J. Lynn, III, *Remarks on Cyber at the RSA Conference*, Feb. 15, 2011, *available at* http://www.defense.gov/speeches/speech.aspx?speechid=1535 (they may also "have the best operational capacity to respond").

[60] OECD, "Proactive Policy Measures by Internet Service Providers against Botnets," OECD Political Economy Paper No. 199, at 8, *available at* http://dx.doi.org/10.1787/5k98tq42t18w-en. For an argument that government should be the entity in control see Jay P. Kesan & Carol M. Hayes, *Thinking Through Active Defense in Cyberspace*, in Proceedings of a Workshop on Deterring CyberAttacks: Informing Strategies and Developing Options for U.S. Policy 334 (2010).

the past. Defense and security at this system point might defuse, at least in part, the debate about how far beyond its own systems a victim can go to defend itself against cyber intrusions. In addition, at this juncture ISP actions rather than government action could mediate the potential threat of government overreach.[61] The same is arguably true of the predictive and learning aspect of a cyber immune system that requires the collection and longitudinal analysis of enormous amounts of potentially personally identifiable information.[62]

The automated nature of a cyber immune system could potentially incorporate actions that would effectuate legal standards and strengthen the protection of civil liberties. An immune defense would automatically identify and disable malicious code and cyber threats based on a reasonable and sufficient level of evidence, but the standard could potentially be less sensitive to attribution questions because it is not applied by a government actor. If an ISP outside of government control undertakes robust action it would probably not be considered an act of a nation state.[63] Establishing a means for redress for mistakes and a waiver of liability for ISPs if actions are taken in good faith and according to reasonable security standards are important considerations.

An automated cyber immune system that is implemented at the ISP level might contribute significantly to national security and property protection while maintaining access and facilitating speech for the community. National security can be strengthened by private actions that increase the security of computers and systems of computers from attack, and ISPs seem to be in a good position to aid in that protection.

If a nation implemented an automated process, then perhaps established levels of technical predictability could form the basis, at least in part, for standardized due process and judicial approval. In addition, the question of intent towards a particular nation, as in an act of war, might be negated if action was taken towards all system threats automatically rather than being an individual decision against a particular nation. This design and implementation might forestall heightened global conflicts.

The discussion leaves detailed comparative analysis of important legal areas such as jurisdiction and electronic communications surveillance [64] for future discussion, but it may be noted that these issues will be resolved differently in unique legal cultures that address important social goals. For example, the recent OECD study

---

61 *See* Michael Chertoff, *Foreward,* 4 Nat'l Security L. & Pol'y 1, 5 (2010).

62 *See* Patriots Debate, *supra* note 57, at 123-134.

63 *See* Scott J. Shackelford & Richard B. Andres, *State Responsibility for Cyber Attacks: Competing Standards for a Growing Problem,* 42 Geo J. Int'l L. 971, 985-88 (2011).

64 See for example, Legal Implications of Countering Botnets, *supra* note 29 (comparing in detail the statutory provisions in Estonia and Germany, for example).

of ISP actions to defeat botnets outlines different approaches of eight countries and notes that future international cooperation will require development of communication between different participants, governmental or ISP.[65] It is highly likely that an immune system design would be different from nation to nation and that communication between systems and nations would be essential.

5. CONCLUSION

The adoption and implementation of a cyber immune system is not an easy technical task; in comparison, the thorny legal and ethical issues across global boundaries are equally daunting. While the automated nature of a cyber defense may present legal challenges to both state and non-state actors, perhaps it can also mitigate the legal ramifications if the system of rules is carefully crafted. The design of the technical system and its implementation should not only secure cyberspace, it should also incorporate legal and ethical principles that will preserve the essential values of a democratic system that are enabled by features of Internet communications.

---

[65] Id.