MALWARE AND DISEASE: LESSONS FROM CYBER INTELLIGENCE FOR PUBLIC HEALTH SURVEILLANCE

Frank L. Smith III

Malicious software and infectious diseases are similar in several respects, as are the functional requirements for surveillance and intelligence to defend against these threats. Given these similarities, this article compares and contrasts the actors, relationships, and norms at work in cyber intelligence and disease surveillance. Historical analysis reveals that civilian cyber defense is more decentralized, private, and voluntary than public health in the United States. Most of these differences are due to political choices rather than technical necessities. In particular, political resistance to government institutions has shaped cyber intelligence over the past 30 years, which is a troubling sign for attempts to improve disease surveillance through local, state, and federal health departments. Information sharing about malware is also limited, despite information technology being integral to cyberspace. Such limits suggest that automation through electronic health records will not automatically improve public health surveillance. Still, certain aspects of information sharing and analysis for cyber defense are worth emulating or, at the very least, learning from to help detect and manage health threats.

DISCOURSE ABOUT CYBERSECURITY is riddled with biological analogies and metaphors. We describe malicious software in terms of “viruses” and “worms,” in part because some of their similarities are significant for security. Most important, contagion of either kind can threaten the community at large. Infectious diseases can spread through travel and trade, as illustrated by the Ebola outbreak in West Africa, Middle East respiratory syndrome, and the H1N1 pandemic, among countless other examples. Like the human ecosystem, the internet is another kind of global network, and malware ranging from Conficker and Zeus to Stuxnet has spread through cyberspace in recent years.

To the extent that malware and infectious diseases are analogous threats, they may warrant similar solutions. In particular, several policy analysts claim that “cyber public health” and “cyber hygiene” would be improved by creating a “cyber CDC,” mirroring the US Centers for Disease

Control and Prevention (CDC), or even a “cyber WHO” modeled on the World Health Organization.¹⁻⁸ “Both public health and cybersecurity aim to achieve a positive state (health or security) in a loosely affiliated but highly interdependent network.”^{9(p77)} While the details differ, some of the functional requirements for achieving cyber and health security are similar as well. Among others, these functions include collecting data about threats to the population (eg, malware or disease), analyzing this information, and reporting to inform action—in a word, surveillance.

What insight does cybersecurity offer for improving public health surveillance, given their family resemblance? Can public health learn from its younger, digital cousin? To answer these questions, this article compares disease surveillance with what is now called cyber intelligence, specifically as it relates to malicious software. The research methodology is described first. Important similarities between malware and infectious disease are identified next,

Frank L. Smith III, PhD, is a Senior Lecturer, Centre for International Security Studies, University of Sydney, New South Wales, Australia.

followed by the functional similarities between disease surveillance and cyber intelligence. The organizational histories of these fields are then compared and contrasted at the local, national, and international levels.

Despite roughly analogous threats and functional requirements, there are striking differences in how these fields are organized. Cyber intelligence is more decentralized, private, and voluntary than disease surveillance in the United States. These differences inform at least 3 lessons for public health policy: (1) the prevailing politics of the time have changed to the detriment of health agencies inside government; (2) electronic health records will not automatically improve disease surveillance; and (3) the CDC could adopt aspects of information sharing and analysis from cyber defense to help improve its image and data exchange. The logic of each lesson is examined in the final discussion.

METHODOLOGY

This article provides a qualitative, historical analysis of cyber intelligence and disease surveillance. It compares and contrasts the actors, relationships, and norms at work in each field. The empirical evidence draws on more than a dozen semistructured interviews with practitioners in public health and cyber defense (30 to 120 minutes in length, tape recorded or written notes, most not for attribution), as well as archival research and existing literature (grey and peer reviewed). While the primary focus is on the United States, international cooperation is also addressed.

ANALOGOUS THREATS: MALICIOUS SOFTWARE AND INFECTIOUS DISEASE

Cybersecurity would be important for public health even if malware and disease were unrelated. The confidentiality, integrity, and availability of health information are vital to this profession and threatened by security challenges ranging from medical data breaches to ransomware targeting hospitals. Of course, it is important to note that malicious software and infectious diseases are not the same. Malware is computer code processed by digital electronics, whereas diseases and their hosts are biological organisms. Malware is not lethal, while infectious diseases kill millions of people each year. Usually, malware is created with malicious intent (as its name implies), but the vast majority of infectious diseases are naturally occurring and lack hostile motives (with the rare exception of biological weapons).¹⁰

Nevertheless, these threats are similar in several ways that are significant for security. First and foremost, both malware and infectious disease can be contagious and widely spread. Transmissibility varies: Not all cyber attacks are

broadcast or intended to spread beyond a specific computer, and not all infectious diseases are contagious. Yet, the potential for spread means that the threat to any individual or computer depends in part on the health of the overall population or network. This interdependence also means that securing either kind of system through intelligence or surveillance depends in part on local, national, and international cooperation.

Second, both malware and disease have nonkinetic effects that can be difficult to detect.¹¹ This difficulty complicates surveillance and source attribution because symptoms can be delayed, hidden, or nonspecific, leaving victims and vectors unaware. Detection, diagnosis, and treatment can therefore require specialized knowledge and tools:

Just as medical researchers have to study a virus before they can create a vaccine, antivirus makers must capture a computer virus, take it apart and identify its “signature”—unique signs in its code—before they can write a program that removes it.¹²

Here again, cooperation is helpful for developing these countermeasures. For example, antivirus companies now share malware samples to improve detection, and the vaccine industry has long benefited from the virus samples shared through the Global Influenza Surveillance and Response System (GISRS).^{13,14}

Both the advantages of cooperation and difficulties of detection are compounded by the variety of malware and disease. New pathogens are always emerging (eg, through antigenic drift and shift in influenza). New malware is also common. According to Symantec, “there were more than 317 million new pieces of malware created” in 2014, “meaning nearly one million new threats were released into the wild each day.”^{15(p7)}

Finally, some of the specialized knowledge and tools used to detect and treat malware and disease are dual use. This means that they can be used for both benefit and harm, or, alternatively, for both military and civilian applications. Cyber intelligence and disease surveillance are both conducted by military and civilian agencies because malware and disease are both interpreted as threats to national security.¹⁶ Furthermore, knowing how to detect malware can be used to help remove it or to hide the code and cause harm. Disease surveillance is rarely thought of in terms of potential harm, since the information it provides is intended to help reduce morbidity and mortality. But this information can also be used to stigmatize and discriminate against individuals and groups, as well as restrict travel and trade. Fear of misuse has fueled resistance to disease surveillance, including popular opposition to name-based reporting of HIV and government opposition to reporting outbreaks such as SARS and H5N1.¹⁷⁻¹⁹ One consequence of these dual-use dilemmas is that cooperation is not inevitable, even when it would be advantageous for cyber or health security.

ANALOGOUS FUNCTIONS: CYBER INTELLIGENCE AND DISEASE SURVEILLANCE

Just as malware and infectious disease are roughly analogous threats, so too are certain aspects of acquiring, interpreting, and communicating information about them. According to the CDC, “Public health surveillance is the ongoing, systematic collection, analysis, interpretation, and dissemination of data regarding a health-related event for use in public health action.”²⁰ Similar terminology is used to define “cyber intelligence”—namely, “the acquisition and analysis of information to identify, track, and predict cyber capabilities, intentions, and activities that offer courses of action to enhance decision making.”^{21(p2)}

Malware is one kind of cyber capability subject to intelligence, as infectious disease is one kind of health-related event—along with noncommunicable diseases, injuries, medical services and devices, and the like—subject to surveillance, biosurveillance, or “health intelligence.”²² And both fields differ from espionage. Following revelations by Edward Snowden, associating the word “cyber” with “intelligence” or “surveillance” may bring to mind warrantless wiretapping, bulk collection of metadata, and other controversial programs conducted by the National Security Agency (NSA). But clandestinely gathering intelligence for counterterrorism differs from collecting, analyzing, and sharing information with consent to improve internet security, just as disease surveillance differs from spying.

As shown in Table 1, similar kinds of information can be collected, analyzed, and shared through cyber intelligence and disease surveillance. First, information about malware includes the source code (human readable) and binary files (machine readable). These files can be summarized as signature or hash functions to help automate detection; they can also be analyzed to identify other indicators of compromise and clues about their author or origin. Second, data on susceptible, infected, and exposed hosts can provide information about vectors and vulnerable computers in the population. Third, cyber intelligence, like disease surveillance, relates to action. Information about defensive action includes the actors involved, as well as how they detect, contain, and remediate threats using patched or recon-

figured software, firewalls, blacklists, access controls, and other countermeasures.

To be clear, computer forensics is not the same as shoe leather epidemiology. At an abstract level, however, cyber intelligence is sufficiently similar to disease surveillance that comparing their respective histories and policies can provide useful insight into each field. Since cyberspace is a relatively new domain, the organizations that have been created to defend it are more sensitive to recent trends in politics and technology than many older institutions in public health. Therefore, cyber intelligence may serve as a sentinel case for the forces that stand to reshape disease surveillance in the years ahead.

COMPARATIVE ANALYSIS: LOCAL, NATIONAL, AND INTERNATIONAL ORGANIZATIONS

The basic structure of disease surveillance at the local, national, and international levels is familiar to many public health professionals. But neither the organizations involved nor their future should be taken for granted. These actors, relationships, and norms look different from those in cyber intelligence, despite similar threats and functional requirements. In addition, politics have had a profound impact on both fields, and the prevailing politics have changed over time.

Origins of Disease Surveillance

American public health consisted mostly of local, uncoordinated, and episodic sanitation and quarantine measures until the bacteriological revolution.²³⁻²⁵ These local roots are still evident in the design of many health departments across the United States. The modern practice of public health surveillance also reflects important political compromises, quite distinct from the germ theory of disease.

Local laws about infectious disease date back to the colonial era, but the proliferation of modern regulations for surveillance coincided with the new science of bacteriology in the 1880s and 1890s. For instance, one of the first bacteriological laboratories in the United States was

Table 1. Parallels Between Information from Cyber Intelligence and Disease Surveillance

<i>Subject</i>	<i>Malicious Software</i>	<i>Infectious Disease</i>
Agents	<ul style="list-style-type: none"> • source code and binaries • signature or hash functions (eg, MD5, SHA) • origin, author, intent 	<ul style="list-style-type: none"> • pathogens (eg, virus samples) • gene sequences • origin, evolution, etc
Vulnerabilities	<ul style="list-style-type: none"> • outdated systems, hostile or compromised IP addresses, domain names, breach details 	<ul style="list-style-type: none"> • susceptible, exposed, infected, and recovered individuals
Defenses	<ul style="list-style-type: none"> • response agencies and officials • detection, containment, remediation 	<ul style="list-style-type: none"> • response agencies and officials • detection, infection control, treatment

established in Michigan in 1888, and “in 1893, Michigan became the first jurisdiction to require the reporting of specific infectious diseases.”^{26,27(p3)} Soon after, laboratory diagnosis became commonplace and compulsory reporting became the norm. “By 1901, all state and municipal laws required notification (i.e., reporting) to local authorities of selected communicable diseases.”^{27(p3)}

Bacteriology “brought professionalism to disease control,” and laboratory diagnosis provided these professionals with newfound “status and authority.”^{17(p3)} However, the political power afforded by this status and authority was insufficient to overcome countervailing interests. “Public health...sought to expand the role of government as a guardian against disease,”^{17(p256)} but many physicians in private practice opposed surveillance as a “demand for unpaid labor” and threat to their clinical authority.^{17(p13)} To win or defuse conflicts of interest over reporting tuberculosis and venereal disease at the turn of the century, public health officials—including outspoken proponents of surveillance such as Hermann Biggs—conceded that they would not encroach on the health care provided through private practice in exchange for notification.

This concession was a political compromise. While it was expedient, limiting the actions that might otherwise have been informed by disease surveillance is hard to justify in terms of maximizing technical efficiency. Nevertheless, this compromise was one of many, and it endures to this day as a practical constraint on the relationship between disease surveillance and local intervention.

Computer Emergency Response Teams

Germ theory revolutionized biology, but cyberspace is man-made and thus somewhat less mysterious (eg, malware was never blamed on miasma or treated with leeches, although scam and snake oil solutions are not uncommon). John von Neumann theorized about self-replicating automata as early as 1949, and Fred Cohen coined the term “computer virus” in 1984, years before malware became a common threat.^{28,29} Instead of a new scientific theory, organizations for civilian cyber defense emerged in response to communication and coordination problems highlighted by the Morris worm.

In November 1988, the Morris worm exploited flaws in the Unix operating system to quickly spread, infecting and slowing about 10% of the 60,000 to 80,000 computers that constituted the entire internet at that time. A few weeks later, another hack compromised the US military’s network. Postmortem reviews of these incidents concluded that response was hampered by limited communication and coordination.³⁰ To address these problems, the Defense Advanced Research Projects Agency (DARPA) funded the Software Engineering Institute at Carnegie Mellon University to establish the Computer Emergency Response Team Coordination Center (CERT/CC).

Naming the CERT/CC a “coordination center” did not mean that the collection, analysis, or dissemination of data about malware and software vulnerabilities were centrally coordinated. The CERT system was a decentralized approach to cyber intelligence. From the beginning, “other agencies and constituencies were encouraged to create and sustain their own teams.”^{31(p19)} These teams typically serve narrow and discrete constituencies (eg, a single company), unlike the local, municipal, and state health departments that serve the entire population in a given location. The result is a loosely coordinated “mosaic of hundreds of independently operating CERTs across the world.”^{32(p92)}

The CERT/CC is not a government agency, in contrast to the health departments that conduct most disease surveillance. Nor can it make or enforce rules. “From the very beginning,” according to one founder of the CERT/CC (interview October 2015), “DARPA stressed... that we had no authority.” Moreover, little capacity for cybersecurity was developed inside local, municipal, or state governments. Even now, fewer than half of local law enforcement agencies have a cybercrime unit.³³ Therefore, unlike other threats to public health and safety, the only recourse that most malware victims have is through a commercial service provider, such as an antivirus vendor like Symantec or McAfee. In sum, in addition to being more decentralized, the United States chose a more private and voluntary approach to cyber defense compared to public health at the local level.

National Institutions for Public Health

Disease surveillance in the United States is a patchwork of state systems, developed through a long political process rather than an inevitable response to contagion. Congress created the US Marine Hospital Service in 1798, but control was not centralized until John Woodworth was appointed the first Surgeon General in 1871. Woodworth “adopted a military model for his medical staff” that was later institutionalized as the commissioned corps of the Public Health Service (PHS).³⁴ He also aimed “to expand the service into a national quarantine agency” and “gather information about the spread of contagious diseases throughout the world.”^{23(p162)} Despite political resistance, the Marine Hospital Service eventually gained control over quarantine through bureaucratic empire-building within the federal government.

Here, as elsewhere, federal authority can be seen as constrained by the Tenth Amendment to the Constitution or empowered by the General Welfare Clause and the Commerce Clause.³⁵ Either way, deference to states’ rights remained the norm for disease surveillance. The PHS appointed epidemiologists to serve in state health departments in 1914, but the federal government did not establish an agency dedicated to disease surveillance until 1946.²⁷

Even then, when the CDC was built on a wartime campaign against malaria, its bureaucratic survival was not assured. “The CDC sometimes encountered opposition from better-established wings of the Public Health Service that resented the intrusion of a newcomer,” and “the National Institutes of Health [NIH] ... also resented the upstart institution in Atlanta,”^{36(p28)} so “the possibility that CDC would be dismantled and merged with NIH was very real.”^{36(p49)} To survive, the CDC sought to distinguish its fieldwork in service to the states from research at NIH. Similarly, Alexander Langmuir cited the threat of biological weapons during the Korean War to justify CDC’s Epidemic Intelligence Service, which was also used to support state and local health officials.¹¹

Service to the states therefore became gospel at CDC, helping it become an authoritative federal agency while still deferring to states’ rights. Prompted by Langmuir at CDC, the Council of State and Territorial Epidemiologists (CSTE) created an annual list of notifiable diseases in 1951. Reporting through the National Notifiable Disease Surveillance System is voluntary and somewhat variable; however, notification is compulsory at the state level, and, “in practice, states do notify the CDC.”^{35(p1038)} Disease surveillance is conducted by other federal agencies as well (eg, the Department of Agriculture, the Food and Drug Administration, and the Department of Defense), but CDC is the dominant authority in this field. It is also the biggest source of public health grant money, and this funding gives the CDC considerable power over the state health departments that it serves (interview with local public health official and former EIS officer, July 2015).

National Cyber Intelligence

There is no national institution for cyber intelligence with the same authority and resources as the CDC. Instead, the CERT system spread alongside a global marketplace—now worth almost \$100 billion—for cybersecurity products and services. These products and services include various forms of threat data and analysis, as well as hardware and software to limit the damage caused by cyber attacks (eg, patches, antivirus, firewalls, encryption, intrusion detection and prevention systems, etc).

How effective is this organizational ecosystem? Paradoxically, while the internet has drastically decreased the cost of communication, limited information is shared about threats to information technology.^{2,3,37-39} Reporting is often ad hoc and idiosyncratic, depending more on interpersonal trust than institutional affiliation. Data collection and analysis are also balkanized.⁴⁰ Unlike epidemiology, where there is some consensus over CSTE case definitions, different vendors and CERTs use different nomenclature to name malware and count its frequency. Consequently, “comparing incident statistics across teams is difficult and often meaningless,” which diminishes the value of what little information is shared.^{31(p83)}

Proposals for the federal government to establish authoritative standards and agencies have gained little traction. In 1989, the General Accounting Office (GAO) argued that internet security required a focal point. It proposed that the Office of Science and Technology Policy (OSTP) establish this focal point, but to no avail.³⁰ In 1991, the National Research Council recommended that the government help establish a nongovernmental organization to serve a similar function—again, with no apparent impact.⁴¹ CERT/CC even pitched a similar proposal in 1997, which, by implication, was a concession that the CERT/CC had failed to establish itself as the single clearinghouse for cyber intelligence.⁴²

In 1998, President Bill Clinton issued Presidential Decision Directive 63 (PDD-63),⁴³ calling for “A Public-Private Partnership” to reduce the vulnerability of critical infrastructure to cyber attack. PDD-63 encouraged the private sector to create an Information Sharing and Analysis Center (ISAC), modeled on the CDC:

As ultimately designed by private sector representatives, the ISAC may emulate particular aspects of such institutions as the Centers for Disease Control and Prevention that have proved highly effective. ...⁴³

However, unlike the CDC (ie, a federal agency with police powers, informed by compulsory reporting at the state level), this ISAC was to be private and voluntary. Moreover, “the single ISAC—the one PDD-63 calls for—was never built” (interview with former US National Security Council staff, September 2015). Rather than establish a single clearinghouse, building separate ISACs became a business opportunity.⁴⁴ At least 19 sector-specific ISACs were subsequently established for financial services, energy, healthcare, and other parts of critical infrastructure. While reasonable, this outcome was not inevitable, especially since variation inside a given sector (eg, small and medium enterprises versus multinational corporations) may be just as significant for security as variation across sectors (eg, finance versus energy or healthcare).

The Department of Homeland Security (DHS) was created in the aftermath of September 11, and it built capacity for cyber intelligence through the United States Computer Emergency Readiness Team (US-CERT) and the National Cybersecurity and Communications Integration Center (NCCIC). In the future, the NCCIC or US-CERT may come to resemble the CDC. Yet, the CDC started out with hundreds of employees.⁴⁵ US-CERT started out with a few dozen people and a small room, “with one table and one chair in one corner” (interview with CERT/CC staff, October 2015).⁴⁶ Today, the CDC provides more than \$3 billion per year in grants for domestic public health, along with more than \$400 million for global health.^{47,48} The Homeland Security Grant Program provides more than \$1 billion to help states counter terrorism and other hazards, but most of this money is spent on physical rather than cyber security (interview with

former MS-ISAC staff, November 2015). In addition, US-CERT was intended to play an international role, and yet it focuses on domestic agencies, with less global engagement than initially imagined (interview with former US-CERT staff, September 2015). Analogous functions and threats aside, national cyber intelligence is structured differently from disease surveillance.

International Differences: FIRST Versus WHO

Less than a year after the Morris worm, the CERT/CC helped the US Department of Energy and the National Air and Space Administration respond to the Wank worm, an early attempt at antinuclear hacktivism that protested the plutonium-powered Galileo spacecraft in 1989. Initial signs pointed to France and then Australia, and this incident fueled interest in international information sharing.⁴⁹ CERT/CC therefore helped create the Forum of Incident Response and Security Teams (FIRST) in 1990.

FIRST provides “access to best practices, tools, and trusted communication.”⁵⁰ It started out as a small club (except for 1 French team, the other founding members were all American).³¹ It has since grown into an international forum for more than 300 national and industry teams from around the world. Given this international membership, FIRST can be compared with the World Health Organization. As with comparisons between CERTs, ISACs, and the CDC, however, FIRST is no WHO.

Unlike the WHO, FIRST did not build on previous international organizations. FIRST was the first of its kind. In contrast, the WHO was preceded by several international organizations and false starts, including the Pan American Sanitary Bureau (PASB), the Office International d’Hygiene Publique, and the Health Organization of the League of Nations. The structure of WHO reflects the politics of this legacy. For example, PASB leveraged its existing status to maintain autonomy and resist full integration into the WHO in 1948, a political precedent that helped other regional offices lock in similar arrangements and authorities.^{51,52}

Furthermore, FIRST did not build on international law. In contrast, WHO administers the International Health Regulations (IHR), the origins of which trace back to the 19th century. After decades or more of noncompliance with these legally binding regulations, the IHR were revised in 2005. The revised IHR require member states to report all public health events of international concern, and they authorize WHO to acknowledge unofficial information about these events. In theory, WHO can use this authority to “name and shame” noncompliance (even though it rarely does so, bowing instead to political pressure from member states, and noncompliance persists).^{52,53} However, “FIRST exercises no authority over the organization and operation of individual member teams.”⁵⁴ It does not pretend to be an operational agency or wield international law.

FIRST merely consists of a small board, a few committees, and an annual conference. It is dwarfed by WHO, which has a \$4 billion budget and oversight of surveillance through programs such as GISRS and the Global Public Health Intelligence Network (GPHIN). As small as FIRST appears in this comparison, it is still more prominent than other international organizations involved with cyber intelligence. For instance, the International Multilateral Partnership Against Cyber Threats (IMPACT) is supposedly “modelled after the Centers for Disease Control and Prevention ... to enhance the global community’s capabilities in dealing with cyber threats.”⁵⁵ But IMPACT has little following or credibility in advanced industrialized countries (interview with former AusCERT staff, May 2015). Here again, this international ecosystem looks very different from disease surveillance.

POLICY DISCUSSION

The institutional differences between disease surveillance and cyber intelligence are striking. On balance, cyber defense is more private, voluntary, and decentralized than public health. Which field is more effective is beyond the scope of this study, and “there is no simple relationship between central control and effective surveillance.”^{22(p1071)} Nevertheless, the chorus of criticism surrounding cyber defense suggests that public health may have the advantage. Either way, the history of cyber intelligence provides at least 3 important lessons for disease surveillance.

American Politics Drives Public Policy

First, both fields reflect political choices at least as much as any technological imperative. For example, in public health, the power and interests of physicians in private practice constrain the potential for local intervention informed by disease surveillance. The CDC’s service—or federal deference—to states is a political choice as well, as is the patchwork of different state systems. “US public health law and policy are inescapably political,” and they have been “from their very inception.”^{56(p46)} The same is true for global health governance.

Cyber intelligence is also shaped by politics, particularly the American ideology of “anti-statism.”⁵⁷ Ideological opposition to government institutions and interventions was ascendant during the 1980s and 1990s, at the same time that cyberspace and network threats were coming online. Anti-statism was bipartisan: The debate was less over whether to cut government and more over how much to cut. Thus, it was politically infeasible to provide cyber intelligence as a public good or service through government. This ideology helps explain why civilian cyber defense is now more decentralized, private, and voluntary than public health.

Things could have been different. After all, the internet was born on public infrastructure with military funding. The United States could have built a focal point for cyber intelligence inside the government, like the CDC. For better or worse, it could have worked through an inter-governmental organization such as the International Telecommunications Union, which, like the WHO, is part of the United Nations (UN). Instead, the United States chose to rely on CERTs, ISACs, FIRST, and other private sources for cyber intelligence. The 1980s and 1990s were not the 1940s, when the United States had been willing to build government agencies at home (eg, CDC) and abroad (eg, the UN and the WHO). The ideological pendulum had swung towards anti-statism, and cyber intelligence reflects this shift in the marketplace of ideas.

Cyber intelligence therefore provides a cautionary tale for public health. As underfunded and uncoordinated as disease surveillance may be, it could be worse. If the CDC did not already exist, it would be difficult to build this kind of government agency in this day and age. Building the WHO would be even harder. Path dependency suggests that the CDC and the WHO will survive, but they should not be taken for granted. More important, if these agencies are going to help improve disease surveillance, then their policies and actions must be politically sophisticated, given the prevailing ideology in the United States. Without this kind of leadership, progress is unlikely.

Information Technology Is No Panacea

A second lesson to learn from cyber intelligence is that information technology does not guarantee information sharing. Electronic records are native to the internet, as are the means to share them (email, listserv, web portals, etc). But information sharing about malware and other cyber threats remains limited, which, in turn, limits how much “big data” is available and amenable to analysis. Sometimes, critical information is not even shared with potential victims. For example, IP addresses infected by the Conficker worm are routinely identified without informing the users of these compromised systems or removing the malware.¹³ This practice may break with sound medical ethics for diagnosing and treating disease (although it pales in comparison to the infamous Tuskegee experiments). Either way, the lack of information sharing is not due to any lack of information technology.

Therefore, as revolutionary as information technology and electronic health records may be for disease surveillance, they are no panacea. The technical challenges of moving from manual to automated data management are easy when compared to the political barriers to sharing information through interoperable systems. These barriers range from conflicts between public and private interests to privacy and liability concerns derived from the dual use of data, all of which have contributed to the balkanization of cyber intelligence.

Public health officials should work to avoid similar fragmentation. To this end, it is important to recognize how the design and implementation of electronic records are not merely functions of technical efficiency but rather choices with distributional consequences (ie, there are winners and losers). One potential advantage for public health agencies is that disease surveillance is “hierarchical and relatively simple in structure.”^{58(p2)} This structure places CDC and the Department of Health and Human Services (HHS) in a strong bargaining position to promote open standards for information sharing (including common nomenclature and data types). If harmonized, these standards can create network effects—namely, positive externalities—that substantially increase the volume and value of information available. So, in addition to modernizing the National Electronic Disease Surveillance System (NEDSS), the CDC and HHS should aggressively push the development and adoption of data standards, as well as “meaningful use” criteria for electronic health records to include public health.⁵⁹

Cyber Intelligence Isn't All Bad

Finally, while cyber intelligence leaves much to be desired, some aspects of this field may be worth replicating. After all, the relatively hierarchical system whereby state health departments report information to the CDC is not above reproach. The CDC can be criticized for being a black box into which information flows “but does not come back.” Ironically, this criticism echoes what some cybersecurity experts say about sharing information with intelligence agencies like the NSA. Given that the politics of American anti-statism resist increasing federal administration of public health surveillance, alternative approaches for improving collection, analysis, and reporting also warrant consideration.

Because ISACs for cyber intelligence failed to actually emulate the CDC, one alternative approach would be for the CDC to sponsor an ISAC for public health surveillance.⁶⁰ The CDC Office of Public Health Scientific Services could seed this public-private partnership, which might look like the National Health Information Sharing and Analysis Center (NH-ISAC) for cybersecurity in the healthcare sector. Ideally, it would combine the lessons learned from NH-ISAC with experience from CDC's pilot fusion center, BioPHusion.⁶¹ Likewise, private sector participation may help this ISAC avoid some of the problems suffered by the DHS National Biosurveillance Integration Center.⁶²

The goals would be consistent with the CDC's surveillance strategy.⁶³ The ISAC could help make surveillance “more adaptable to the rapidly changing technology landscape” by allowing tech vendors and users to engage in an operational environment on an ongoing basis.⁶³ It could help make surveillance “more versatile in meeting demands for expanding knowledge about evolving threats to health”⁶³ by providing a sanctioned forum for stakeholders to share and

evaluate heterogeneous data alongside internet-based surveillance (GPHIN, HealthMap, ProMED, etc), official sources (eg, NEDSS, Epi-X), and similar systems. The ISAC could also help make surveillance “more able to meet the demands for timely and ... [specific] information”—especially demands from outside the CDC—by broadening participation.⁶³

Of course, the devil is in the details, and an ISAC cannot replace surveillance by local, state, and federal authorities (a lesson that may be dawning on cybersecurity experts). This article provides a foundation for further research, and an ISAC for public health surveillance may be found to complement the existing architecture. Even if the CDC rejects this particular approach, it can still learn from the successes and failures of cyber intelligence. This field is in touch with information technology, by definition. It is sensitive to contemporary politics, lacking the longer legacy of public health. Therefore, while cyber intelligence and disease surveillance are not the same, the threats and functional requirements are too similar to ignore when crafting better policy.

ACKNOWLEDGMENTS

The author wishes to thank the interview respondents who contributed to this research, the Institute for Security and Conflict Studies, and, for helpful feedback, Rebecca Katz, as well as the editors and anonymous reviewers of *Health Security*.

REFERENCES

- Geer D. Cybersecurity as realpolitik. August 6, 2014. <http://geer.tinho.net/geer.blackhat.6viii14.txt>. Accessed July 12, 2016.
- Singer PW, Friedman A. *Cybersecurity and Cyberwar: What Everyone Needs to Know*. New York: Oxford University Press; 2014.
- Singer PW. How to save the net: a CDC for cybercrime. *Wired* August 19, 2014. <http://www.wired.com/2014/08/save-the-net-peter-singer/>. Accessed July 12, 2016.
- Rowe J, Levitt K, Hogarth M. Towards the realization of a public health model for shared secure cyber-space. *Proceedings of the 2013 Workshop on New Security Paradigms*. 2013. <http://web.cs.ucdavis.edu/~rowe/papers/NSPW%202013%20-%20RoweLevittHogarth.pdf>. Accessed July 12, 2016.
- Charney S. Collective defense: applying the public-health model to the internet. *IEEE Security & Privacy* 2012;10(2):54-59.
- Sullivan K. *The Internet Health Model for Cybersecurity*. New York: EastWest Institute; 2012.
- Sauver JS. We need a cyber CDC or a cyber World Health Organization. Anti-Phishing Working Group Counter e-Crime Summit; May 31, 2007; San Francisco, CA. <https://www.stsauver.com/~joe/ecrime-summit/ecrime-summit.pdf>. Accessed July 12, 2016.
- Rice M, Butts J, Miller R, Sheoni S. Applying public health strategies to the protection of cyberspace. *International Journal of Critical Infrastructure Protection* 2010;3(3):118-127.
- Mulligan DK, Schneider FB. Doctrine for cybersecurity. *Daedalus* 2011;140(4):70-92.
- Koblentz GD, Mazanec BM. Viral warfare: the security implications of cyber and biological weapons. *Comparative Strategy* 2013;32(5):418-434.
- Smith FL III. *American Biodefense: How Dangerous Ideas about Biological Weapons Shape National Security*. Ithaca, NY: Cornell University Press; 2014.
- Perlroth N. Outmaneuvered at their own game, antivirus makers struggle to adapt. *New York Times* December 31, 2012.
- Schmidt A. *Secrecy Versus Openness: Internet Security and the Limits of Open Source and Peer Production* [PhD thesis]. Delft University of Technology; 2014. <https://www.intgovforum.org/cms/documents/best-practice-forums/establishing-and-supporting-computer-emergency-response-teams-certs-for-internet-security/417-secrecy-versus-openness-internet-security-and-the-limits-of-open-source-and-peer-production/file>. Accessed July 12, 2016.
- World Health Organization. Global Influenza Surveillance and Response System (GISRS). http://www.who.int/influenza/gisrs_laboratory/en/. Accessed July 12, 2016.
- Symantec. Internet security threat report. 2015. https://www.symantec.com/content/en/us/enterprise/other_resources/21347933_GA_RPT-internet-security-threat-report-volume-20-2015.pdf. Accessed August 18, 2016.
- The White House. *National Security Strategy*. February 2015. https://www.whitehouse.gov/sites/default/files/docs/2015_national_security_strategy.pdf. Accessed July 12, 2016.
- Fairchild AL, Bayer R, Colgrove J. *Searching Eyes: Privacy, the State, and Disease Surveillance in America*. Berkeley, CA: University of California Press; 2007.
- Pomfret J. Underreporting, secrecy fuel SARS in Beijing, WHO says. *Washington Post* April 17, 2003.
- Sipress A. Indonesia neglected bird flu until too late, experts say. *Washington Post* October 20, 2005.
- German RR, Lee LM, Horan JM, Milstein RL, Pertowski CA, Waller MN; Guidelines Working Group Centers for Disease Control and Prevention (CDC). Updated guidelines for evaluating public health surveillance systems: recommendations from the Guidelines Working Group. *MMWR Recomm Rep* 2001;50(RR-13):1-35.
- Townsend T, Ludwick M, McAllister J, Mellinger AO, Sereno KA. *SEI Emerging Technology Center: Cyber Intelligence Tradecraft Project. Summary of Key Findings*. Software Engineering Institute, Carnegie Mellon University; 2013. <http://www.sei.cmu.edu/library/assets/whitepapers/citp-summary-key-findings.pdf>. Accessed July 12, 2016.
- Morse SS. Global infectious disease surveillance and health intelligence. *Health Aff (Millwood)* 2007;26(4):1069-1077.
- Duffy J. *The Sanitarians: A History of American Public Health*. Urbana: University of Illinois Press; 1992.
- Fee E, Brown TM. The unfulfilled promise of public health: déjà vu all over again. *Health Aff (Millwood)* 2002;21(6):31-43.

25. Turnock BJ, Atchison C. Governmental public health in the United States: the implications of federalism. *Health Aff (Millwood)* 2002;21(6):68-78.
26. Rosen G. *A History of Public Health*. 2d ed. Baltimore, MD: Johns Hopkins University Press; 1993.
27. Thacker SB, Qualters JR, Lee LM; Centers for Disease Control and Prevention (CDC). Public health surveillance in the United States: evolution and challenges. *MMWR Supp* 2012;61(3):3-9.
28. Cohen F. Computer viruses: theory and experiments. 1984. <http://web.eecs.umich.edu/~aparaksh/eecs588/handouts/cohen-viruses.html> Accessed July 12, 2016.
29. Von Neumann J. *Theory of Self-Reproducing Automata*. Burks AW, ed. Urbana, IL: University of Illinois Press; 1966.
30. US Government Accountability Office. *Computer Security: Virus Highlights Need for Improved Internet Management*. 1989. <http://www.gao.gov/products/IMTEC-89-57>. Accessed July 12, 2016.
31. Killcrece G, Kossakowski K-P, Ruefle R, Zajicek M. *State of the Practice of Computer Security Incident Response Teams (CSIRTs)*. Carnegie Mellon University; 2003. http://resources.sei.cmu.edu/asset_files/TechnicalReport/2003_005_001_14204.pdf. Accessed July 12, 2016.
32. DeNardis L. *The Global War for Internet Governance*. New Haven, CT: Yale University Press; 2014.
33. *The Role of Local Law Enforcement Agencies in Preventing and Investigating Cybercrime*. Washington, DC: Police Executive Research Forum; 2014. http://www.policeforum.org/assets/docs/Critical_Issues_Series_2/the%20role%20of%20local%20law%20enforcement%20agencies%20in%20preventing%20and%20investigating%20cybercrime%202014.pdf. Accessed July 12, 2016.
34. Commissioned Corps of the US Public Health Service. History. <http://www.usphs.gov/aboutus/history.aspx>. Accessed July 12, 2016.
35. Katz R, Rosenbaum S. Challenging custom: rethinking national population surveillance policy in a global public health age. *J Health Polit Policy Law* 2010;35(6):1027-1055.
36. Etheridge EW. *Sentinel for Health: A History of the Centers for Disease Control*. Los Angeles: University of California Press; 1992.
37. Langevin JR, McCaul MT, Charney S, Raduege H. *Cybersecurity Two Years Later*. Washington, DC: Center for Strategic and International Studies; 2011.
38. US Government Accountability Office. *Critical Infrastructure Protection: Key Private and Public Cyber Expectations Need to Be Consistently Addressed*. July 2010. <http://www.gao.gov/assets/310/307222.pdf>. Accessed July 12, 2016.
39. US Department of Homeland Security, Office of Inspector General. *U.S. Computer Emergency Readiness Team Makes Progress in Securing Cyberspace, but Challenges Remain*. 2010. http://web.archive.org/web/20100705034034/http://www.dhs.gov/xoig/assets/mgmttrpts/OIG_10-94_Jun10.pdf. Accessed July 12, 2016.
40. Mundie DA, McIntire DM. *The MAL: A Malware Analysis Lexicon*. Technical Note, CERT Program, SEI, Carnegie Mellon University; 2013. http://resources.sei.cmu.edu/asset_files/technicalnote/2013_004_001_40250.pdf. Accessed July 12, 2016.
41. System Security Study Committee, Commission on Physical Sciences, Mathematics, and Applications, National Research Council. *Computers at Risk: Safe Computing in the Information Age*. Washington, DC: National Academy Press; 1991.
42. Ellis J, Fisher D, Longstaff TA, Pesante L, Pethia RD. Report to the President's Commission on Critical Infrastructure Protection. CERT Coordination Center, Software Engineering Institute; 1997. <http://resources.sei.cmu.edu/library/asset-view.cfm?assetid=12731>. Accessed July 12, 2016.
43. The White House. Presidential Decision Directive/NSC-63. Critical Infrastructure Protection. May 22, 1998. <http://fas.org/irp/offdocs/pdd/pdd-63.htm>. Accessed July 12, 2016.
44. SAIC to acquire security intelligence services from Predictive Systems. *PRNewswire* April 21, 2003. <http://www.prnewswire.com/news-releases/saic-to-acquire-security-intelligence-services-from-predictive-systems-70885632.html>. Accessed July 12, 2016.
45. Centers for Disease Control and Prevention. Our history – our story. 2013. <http://www.cdc.gov/about/history/>. Accessed July 12, 2016.
46. US Department of Homeland Security, Office of Inspector General. *Progress and Challenges in Securing the Nation's Cyberspace*. 2014. https://www.oig.dhs.gov/assets/Mgmt/OIG_CyberspaceRpt_Jul04.pdf. Accessed July 12, 2016.
47. Centers for Disease Control and Prevention: Fiscal Year 2014 Grants Profile Report for U.S. States and District of Columbia. 2014. http://wwwn.cdc.gov/fundingprofiles/Report_Docs/PDFDocs/Rpt2014/All-US-States-By-State-2014-CDC-Grants-Profile-Report.pdf. Accessed July 12, 2016.
48. Centers for Disease Control and Prevention. Budget Request Summary—Fiscal Year 2015. 2014. <http://www.cdc.gov/budget/documents/fy2015/fy-2015-budget-request-summary-and-detail-table.pdf>. Accessed July 12, 2016.
49. Dreyfus S, Assange J. *Underground: Tales of Hacking, Madness, and Obsession on the Electronic Frontier*. Melbourne: Canongate; 1997.
50. FIRST. FIRST vision and mission statement. 2003. <http://www.first.org/about/mission>. Accessed July 12, 2016.
51. Hanrieder T. The path-dependent design of international organizations: federalism in the World Health Organization. *European Journal of International Relations* 2015;21(1):215-239.
52. Kamradt-Scott A. *Managing Global Health Security: The World Health Organization and Disease Outbreak Control*. New York: Palgrave Macmillan; 2015.
53. Cheng M. UKs attempts to stop H1N1 flu called flawed. *Associated Press* May 22, 2009. <http://www.ctvnews.ca/u-k-s-attempts-to-stop-h1n1-flu-called-flawed-1.400947>. Accessed July 12, 2016.
54. FIRST. FIRST Organization. <http://www.first.org/about/organization>. Accessed July 12, 2016.
55. IMPACT. Mission & vision. <http://www.impact-alliance.org/aboutus/mission-&-vision.html>. Accessed July 12, 2016.
56. Goldberg DS. Against the very idea of the politicization of public health policy. *Am J Public Health* 2012;102(1):44-49.
57. Friedberg AL. *In the Shadow of the Garrison State: America's Anti-Statism and Its Cold War Grand Strategy*. Princeton, NJ: Princeton University Press; 2000.
58. Morse SS. Public health disease surveillance networks. *Microbiol Spectr* 2014;2(1):OH-0002-2012.
59. Toner ES, Nuzzo JB, Watson M, et al. Biosurveillance where it happens: state and local capabilities and needs. *Biosecure Bioterror* 2011;9(4):321-330.

60. Lewis N, Campbell MJ, Baskin CR. Information security for compliance with select agent regulations. *Health Secur* 2015;13(3):207-218.
61. Khan AS, Fleischauer A, Casani J, Groseclose SL. The next public health revolution: public health information fusion and social networks. *Am J Public Health* 2010;100(7):1237-1242.
62. US Government Accountability Office. *Biosurveillance: Challenges and Options for the National Biosurveillance Integration Center*. September 2015. <http://www.gao.gov/assets/680/672732.pdf>. Accessed July 12, 2016.
63. Centers for Disease Control and Prevention. *Surveillance Strategy*. 2014. <http://www.cdc.gov/ophss/docs/cdc-surveillance-strategy-final.pdf>. Accessed July 12, 2016.
- Manuscript received December 31, 2015; accepted for publication May 24, 2016.*

Address correspondence to:
Frank L. Smith III, PhD
Centre for International Security Studies
Department of Government and International Relations
Merewether Building (H04), Room 380
University of Sydney
Sydney, New South Wales 2006
Australia

Email: frank.smith@sydney.edu.au