# 11 The Biases of Information Security Research

**Ronald J. Deibert**

Information and communication technologies now pervade, and are critical to the functioning of, every activity on earth.[1] Securing information technologies has, as a consequence, become a major public policy issue. But *how* to secure information and communication technologies is deeply contested (Deibert 2017). The choices that are made to secure information ultimately shape our communications spaces and, by extension, how we secure our societies.

Research on information security is, therefore, critical to navigating this issue in an informed and systematic way. But what is a problem in information security that should be addressed by research in the first place? On first consideration it may seem obvious that the security of information systems is a technological issue and that eventually, with enough systematic attention to engineering of information systems, we can settle on a way to secure information that achieves consensus.

But approaching information systems through a technical-functional lens obscures the politically contested nature of information security as well as how research on information security itself is influenced by external factors. In this chapter, I outline some of the ways in which information security gets defined as a research problem. My aim is to show how political, economic, and other factors shape the field of information security, including what problems are excluded as much as which are addressed or prioritized. After this analysis, it will be clearer how the field of information security is constructed as a regime or community of practice and the implications this shaping has for society and politics writ large (Adler 2008).

In emphasizing these questions, I am not trying to solve technological problems that plague information security. Rather, I am asking epistemological and methodological questions about the constitution of the field

of information security as it exists today. As Langdon Winner puts it, "It is important to notice not only which decisions are made and how but also which decisions never land on the agenda at all; which possibilities are relegated to the sphere of non-decisions" (Winner 1993, 369). Answering these questions requires studying the past, understanding how the field of information security evolved and where it is headed today, including a consideration of how political and economic forces shape what counts as legitimate areas of inquiry and, as importantly, what does not. In short, it requires a sociology of information security knowledge (see Bourdieu 2004; Pinch and Bijker 1993).

I conclude with some suggestions on how to make research on information security more self-aware, more independent, and more broadly interdisciplinary—values that I hope help militate against biases and unquestioned assumptions.

## The Barriers of Disciplinary Silos

A useful starting point for this inquiry is a reminder that academic fields of inquiry are, themselves, social constructions. These fields are made up of communities of practice that share common principles, rules, languages, methods, and even worldviews. These common traits do not mean that all academics within a particular field or discipline think alike. To the contrary, academic fields—especially those that are healthy—are typically characterized by rigorous debates between competing schools of thought. Notwithstanding their internal differences, however, disciplines create fences around research, commonly referred to as disciplinary silos, which have the effect of channeling inquiry into conventions. These conventions are necessary adaptations to a complex world, which requires specialization and division of labor. The downside of disciplinary silos is that they can encourage myopic thinking while discouraging alternative ways of approaching a topic.

With respect to the field of information security research, the most important disciplinary silo is the one separating the computer and engineering sciences from the social sciences and humanities. Few universities today systematically include engineering and computer science curricula in the social sciences, and vice versa. These disciplinary divisions are compounded by the growing imbalance between the natural sciences, on the one hand, and the social sciences and humanities on the other. Research

into science, technology, engineering, and mathematics (STEM) subjects is growing, mostly on the basis of economic arguments. STEM subjects are considered pathways to employment, innovation, and economic growth, while the social sciences and many humanities are increasingly portrayed as frivolous and financially unrewarding. Whereas STEM subjects receive the majority of government and private sector funding, humanities programs are shrinking or being eliminated altogether in absence of equivalent funding. These trends reinforce existing disciplinary divisions in information security research while also privileging technical approaches to information security problems over broader political and economic considerations.

To be sure, there are exceptions. There are growing subfields dealing with human-computer interaction and user interface design, which draw insights and theories from psychology and sociology to better design information systems. Many social scientists and humanists use methods that rely on computer science techniques for quantitative and qualitative data analysis (see chapter 9 by Cogburn and chapter 10 by Ten Oever, Milan, and Beraldo). Information studies programs are growing into a self-identified iSchool movement in which the academic field of information is envisioned as an interdisciplinary whole. Many iSchools include faculty undertaking research on topics broadly related to information security, such as censorship and surveillance.

Another important exception is the subfield of security economics, spearheaded by Cambridge University professor Ross Anderson (n.d.) and others. Anderson and his growing cohort of colleagues examine the incentive structures that shape information security practices, particularly within software and other technology industries. Since most of the IT sector is self-regulated, with competitive dynamics rewarding early innovators, companies have few incentives to invest in protection from the ground up, meaning that those responsible for producing information systems pass on the costs of security to the end user or other parties. As Anderson (2014) explains, "Information economics explain why security is hard: in platform races, winners are likely to be those who ignored security to make life easy for complementers, such as application developers, and they are then likely to use it to lock customers in later rather than just protecting them from the bad guys."

While Anderson's and his colleagues' work bridges STEM and the social sciences, it is incomplete. Although it incorporates economic theory into an

analysis of information security outcomes, it does not examine how political and economic factors may shape what counts as legitimate research into information security in the first place. In other words, it does not extend the analysis of positive and negative incentives into critically examining and reflecting on why the field privileges certain areas of inquiry and methods over others, and what that privileging means for how, and in whose interests, information is secured.

These examples of interdisciplinarity, while encouraging, are still exceptions to strong and well-established conventions. Moreover, there are growing structural constraints that could bias research in ways that reinforce not only those disciplinary conventions but also dominant interests. We turn now to an analysis of some of those structural constraints.

### Structural Constraints on Information Security

Langdon Winner once wrote that "by noticing which issues are never (or seldom) articulated or legitimized, observing which groups are consistently excluded from power, one begins to understand the enduring social structures upon which the most obvious kinds of political power rest" (Winner 1993, 369). What do we notice when we apply this framework to information security? My and my colleagues' research on targeted digital threats at the Citizen Lab provides a compelling example (Citizen Lab 2014). At the Citizen Lab, we have analyzed digital espionage campaigns against civil society groups since 2009. Beginning with our contribution to the landmark *Tracking GhostNet* report (Information Warfare Monitor 2009), and ever since, we have documented persistent cyber espionage campaigns targeting civil society, human rights defenders, political opposition, journalists, and even health scientists. Our conclusion is that the same threat actors—typically government agencies or nonstate actors working on behalf of states—use the same tactics, techniques, and procedures against civil society that they use in espionage campaigns against private sector and government targets. However, civil society typically lacks the resources, support, and capacity to deal with the threat. Defending against digital espionage, from investigation to ongoing remediation, can involve huge investments in money, time, equipment, and personnel that few civil society groups can afford.

Compounding the problem, civil society is not a lucrative client for the multibillion-dollar cybersecurity threat industry. As a consequence, even though private firms may identify civil society targeting in their monitoring

data, there are few fiscal incentives for these companies to follow up and even some potential risks in doing so. While their reporting may list generalized nongovernmental organization (NGO) or civil society targets and victims, those are rarely analyzed in depth. Instead, the reports principally aim to highlight industry and government targets and victims, which are more attractive sources of revenue. These industry reports can then perpetuate misguided assumptions about the actual scope and scale of information security problems, about who is targeted in digital espionage, and why (Maschmeyer, Deibert, and Lindsay 2019; see also Jardine's chapter 7 for other biases in cybersecurity datasets introduced by the private sector).

Meanwhile, a variety of factors militate against policy makers addressing digital espionage against civil society. For many nondemocratic governments, and especially authoritarian regimes, civil society can represent a menace to be co-opted, infiltrated, and neutralized. These governments may see civil society as an information security threat. But even in democratic countries there are few incentives to address this problem. For example, in a 2014 case, a US grand jury indicted five Chinese individuals for "computer hacking, economic espionage and other offenses directed at six American victims in the US nuclear power, metals and solar products industries" (US Department of Justice 2014). Many link the indictment to a subsequent agreement between US President Barack Obama and China's President Xi Jinping to refrain from computer espionage targeting businesses and critical infrastructure (Harold 2016). It is unlikely that equivalent political capital would be marshalled for such an indictment in support of civil society targets. The theft of trade secrets affects jobs, and national security is an existential threat that attracts bipartisan support, but the targeting of Tibetans, human rights NGOs, or journalists does not garner the same political urgency.

This example illustrates how the structures Winner refers to can obscure an important area of information security, in this case the silent epidemic of targeted digital attacks against civil society. Targeted digital attacks on civil society groups tend to be underreported and largely marginalized because, for the private sector cybersecurity threat industry, defending those attacks is not profitable and investments of time or resources cannot easily be justified. For government agencies, the consequences of such attacks rarely rise to the level of a political or economic risk that merits public policy attention. Indeed, a growing number of governments actively target the sector.

Meanwhile, civil society has very little capacity to deal with the problem, creating what is, overall, a failure in the information security market.

A large body of academic research on this area, combined with persistent political advocacy directed at governments and the threat industry, could raise awareness and help address that market failure, which is precisely one of the aims of our research. However, the hurdles standing in the way are numerous and growing.

### A Political Economy of Information Security Research

In a world of billions of networked devices, it may be easy to forget that the Internet began as a relatively small university-based research project. Contrary to the widespread myth of the Internet's origins linking Paul Baran's proposal for a distributed communications system that could survive a nuclear war, the early networking infrastructures that were developed and that evolved into today's Internet were concerned with facilitating time-sharing of scarce computing resources, not just surviving nuclear attack. Engineers focused on enabling network connectivity across nodes and having data flow seamlessly. Security of that network or its communications was not a high priority (Abbate 1999).

It was not until the Morris worm, in 1988, that the threats around network failure and insecurity became more widely noticed and increasingly studied. Researchers began examining how poorly executed code could cause systems to crash or be exploited to cause havoc. Significantly, the lens through which the growing subfield of information security addressed their problems was from a technical-functional one. Research was aimed at highlighting technical weaknesses in information security systems' design to optimize against failure, whether accidental or otherwise.

A technical-functional approach may have been appropriate when information systems were relatively obscure and compartmentalized. But the contemporary information ecosystem, which extends into cultural and political systems across the world, is vastly different from that in which the early innovators worked. The different institutional environments affect what counts as an information security problem in the first place, making the security of information less a *technical* than a *political* issue. Decisions on what problems to resolve, and which issues are not even regarded as problems, are questions of *power*; once those questions are resolved, technical and engineering questions follow along. Practices of information

security, seen as a component of technological production, are thus exercises in the architecture of power. Starting from this perspective can help illuminate what gets priority as an information security research problem and what does not.

## Economic Biases of Information Security Research

The problems for which engineering and computer science solutions are sought and priorities allocated may reflect factors such as the progress of debates in a particular academic field or the evolution of technologies themselves. But they may also reflect the existing power structure of a society and the constraints and opportunities it presents, both directly and indirectly. Among power structures today, economic factors have enormous influence on a wide variety of sectors, academic research among them. For example, it has become increasingly commonplace for universities to justify their programs in terms of an investment in or contribution to the economy. Research programs sell themselves in terms of employment training. This dynamic has positive and negative incentives on research. Positive incentives push for certain problems to be addressed because they are problems for which dominant industries seek creative solutions. For example, social media companies' appetites for better ways of pushing advertisements to their customers on the basis of their online behavior undoubtedly incentivizes researchers to find more efficient ways to monitor users. These incentives can be direct, through financial support, or indirect, in terms of potential postgraduate employment opportunities.

Negative incentives dissuade researchers from looking into certain areas of inquiry because doing so may jeopardize those employment opportunities or risk some kind of legal or other penalty. Examples include undertaking research into security flaws or privacy violations associated with large prospective employers. Who wants to interrogate a hidden and prejudiced algorithm if it will invoke the wrath of a company's powerful legal department or blacklist graduates from prospective jobs?

Negative incentives may affect the choice of research methods as well. For example, reverse engineering software—a method used widely to undertake research on software—may infringe on copyright or intellectual property laws, such as section 1201 of the US Digital Millennium Copyright Act or the US Computer Fraud and Abuse Act. Such laws effectively shackle

certain modes of inquiry by shielding code and networks from outside scrutiny. While protecting business secrets may be the official justification for keeping code hidden, there may be other, political, reasons as well.

For example, in numerous investigations our research group has shown that many popular China-based applications contain hidden censorship and surveillance mechanisms that the developers have engineered to comply with their understanding of government regulations. The research provides an invaluable insight into China-based information controls on popular chat, video-streaming, and gaming applications and how user security and privacy is subordinated to comply with regime security. But none of the research would be possible without our researchers reverse engineering the applications, in some cases breaking their encryption, to discover what algorithms lie beneath the surface. A strict interpretation of intellectual property laws could chill this research, especially if the companies under scrutiny are litigious.

These concerns are not just hypothetical. Our group has been the subject of legal threats in at least three instances by companies who were the subjects of our research. In 2014, the security company Hacking Team experienced a massive data breach. Those responsible leaked the stolen data to WikiLeaks, where it was published online in searchable form. Citizen Lab had published several reports on how the company's products were used by autocratic regimes to target human rights defenders, journalists, and members of political opposition parties; these reports were widely covered in the media and generated negative publicity for the company. A search of their corporate emails as archived on WikiLeaks showed that executives reviewed the letters we sent to the company before we published reports, in which we asked questions about company practices, and that they engaged formal legal advice to "hit CL [Citizen Lab] hard" (Lou 2015).

As a component of research into a deep packet inspection system manufactured by the company Sandvine and its use in Turkey, Syria, and Egypt to redirect unwitting users to spyware and other malicious traffic, Citizen Lab researchers purchased a secondhand Sandvine PacketLogic device from an online commerce site (Marczak et al, 2018). We set up the device in a laboratory to understand its operation and refine the fingerprints we used as part of our network measurement methodology. Before publication, we sent Sandvine a letter describing our research and asking questions about its use in the country contexts. Sandvine threatened legal action against

the University of Toronto if the device was not immediately returned. The University of Toronto denied the request, and the publication proceeded in spite of the threat of legal action.

While Hacking Team and Sandvine did not actually launch legal action, another company did. Netsweeper became notorious after several Citizen Lab reports showed that the company's Internet filtering technology was enabling national-level censorship in several countries, including of political and social content. The company filed a $3.5 million defamation suit against me, as director of the Citizen Lab, and the University of Toronto, over comments made to the media about a Citizen Lab report on Netsweeper's services to Yemen. Canada has historically proved a plaintiff-friendly environment for defamation cases. However, on November 3, 2015, the legal landscape shifted in Ontario when a new law called the Protection of Public Participation Act (PPPA) came into force. It was specifically designed to limit strategic litigation against public participation, or SLAPP, suits. In our view, the work of Citizen Lab, including the research on Netsweeper, was precisely the sort of activity recognized as meriting special protection under the PPPA. Had our proceedings gone forward, we intended to exercise our rights under the act and move to dismiss Netsweeper's action. Ultimately, however, Netsweeper discontinued its defamation suit in its entirety. Regardless, the case underscores the threats to controversial security research that can come from the private sector as well as the types of legal remedies that may protect researchers who engage in that controversial research. I return to this topic in the conclusion.

## Private Sector Gatekeepers on Information Security Research

Our information environment is mediated by large technology companies. These companies control massive repositories of data that are relevant to information security issues, from protection of privacy to censorship and surveillance, to the circulation of state disinformation campaigns, or to efforts to further violent radical extremism. They are also extraordinary potential opportunities as datasets for researchers to interrogate. Indeed, going further than describing these as mere opportunities, it is perhaps better to describe access to such data as a research *imperative*. The less researchers know about how these data are collected, analyzed, produced, and used to shape and limit users' communications experiences, the less they can

authoritatively claim to know about what are arguably some of the most important information security issues of the day.

But what are the conditions of access? Who can access the data and under what terms? As Lev Manovich (2011, 464) notes, "Only social media companies have access to really large social data—especially transactional data. An anthropologist working for Facebook or a sociologist working for Google will have access to data that the rest of the scholarly community will not." Apart from companies publishing only data or research they believe is in line with their for-profit aims, this privatization of core sociological research data may have several consequences for information security research. As boyd and Crawford explain,

> Some companies restrict access to their data entirely; others sell the privilege of access for a high fee; and others offer small data sets to university-based researchers. This produces considerable unevenness in the system: those with money—or those inside the company—can produce a different type of research than those outside. Those without access can neither reproduce nor evaluate the methodological claims of those who have privileged access. (2011, 22)

Researchers who want to work on datasets controlled by companies have some options. Some companies provide access to portions of the data, and many researchers have made use of this access to undertake pathbreaking research. But typically this access is restricted to slices of data or comes with subscription fees to larger, or even complete, datasets. Segregating access to data in this way reinforces all the usual resource inequities that are found across societies: better-resourced departments and universities acquire more and better access than those that are less endowed. This division reinforces long-standing inequities not only across disciplines but across the world, and in particular for researchers in the global South.

The desire to access data may also influence the topics on which researchers choose to focus. Companies may encourage access on the basis of having researchers tackle problems that companies need to solve and, conversely, discourage questions that affect them adversely. As boyd and Crawford (2011, 674) point out, "Big Data researchers with access to proprietary data sets are less likely to choose questions that are contentious to a social media company…if they think it may result in their access being cut."

The influence of private sector and economic factors biasing information security research is likely to grow, as industry becomes a more important sponsor of university-based research. According to a report from the US

National Science Foundation, from 2011 to 2014 federal funds for university research fell to $37.9 from $40.8 billion, while during the same period industry-sponsored university research grew from $4.9 to $5.9 billion.[2]

Although biases introduced into university-based research from the private sector are definitely not unique to information security, the area does have special considerations that bear on the topic. All things being equal, large social media companies and other large technology providers would benefit by a more narrowly defined version of security that focuses largely on technical matters. Companies whose business model rests on surveillance of users' online behavior are unlikely to sponsor research that undermines that model or helps users become aware of just how much they are giving away. These incentives privilege a certain narrow definition of what counts as information security, one in which user privacy is not included.

Companies will also not likely look favorably on research that highlights collusion with governments on lawful access requests or implementation of surveillance or censorship of users, which unfortunately is a growing norm among countries worldwide (Deibert and Crete-Nishihata 2012). A comparison of the full range of state cybersecurity policies would show fairly wide variation in what counts as requiring securing and what practices are facilitated or encouraged by the policies that are adopted. National-level policies have knock-on effects: on companies, consumer behavior, and to a large degree, academic research. For example, China's cybersecurity laws require companies to police their networks, censor forbidden topics, monitor their users, and store their customer data on China's territory, to be available to authorities upon request. Naturally, the laws affect how products are designed, engineered, and effectively secured. They incentivize engineering puzzles to be solved and priorities to be addressed. Research resources are directed accordingly: perhaps to find ways to better monitor users' devices and online behavior or develop ways to restrict their access to information in a manner that is increasingly opaque to users and researchers.

An intriguing and disturbing example concerns research into artificial intelligence (AI). The Chinese government's "Next Generation Artificial Intelligence Development Plan" links AI to China's so-called social credit system—a system whose aim is to combine a comprehensive analysis of users' online behavior with a kind of citizenship score. Major Chinese social media companies, like Baidu and Tencent, all of which engineer extensive censorship and surveillance into their products, have invested heavily in

AI research labs. A 2017 article in *The Atlantic* describes one Hong Kong University–based researcher's collaboration with the company Tencent:

> The students get access to mountains of data from WeChat, the messaging app from Tencent that is akin to Facebook, iMessage, and Venmo all rolled into one. ("With AI, they can't do it without a lot of data and a platform to test it on," says Yang, which is why industry collaboration is so key.) In return, Tencent gets a direct line to some of the most innovative research coming out of academic labs. And of course, some of these students end up working at Tencent when they graduate. (Zhang 2017)

As government pressures to control information bear down heavily on the private sector, both positive and negative incentives faced by firms are invariably passed down to research communities, particularly as industry support for university research increases. On balance, these pressures work to squeeze out spaces for information security research on censorship, surveillance, lawful access, and privacy.

### National Security Biases

The control of information has long been a central ingredient of state power. States have used information to control their domestic populations or project power abroad, through forms of propaganda or information operations. Today, the global information environment sees struggles between states, as well as nonstate actors such as private companies, NGOs, and violent extremists. Within this multifaceted arena of struggle, numerous practices of information security, in turn, can put pressure on and shape information security research. While the previous section highlights some indirect influences of national security via the private sector, in this section we examine some direct impacts.

The most important direct tension between national security and university-based information security research is that between openness and secrecy. Openness is one of the most important foundations for scientific work and is essential for collaboration, peer review, transparency, reproducibility of research results, and public awareness and accountability. Openness prevents myopic thinking, dogmatism, and the spread of misinformation or disinformation. To be sure, there are times when openness is justifiably limited—to protect research subjects' confidentiality, for example—but these are rare exceptions (Resnik 2007).

Just as openness is fundamental to academic research, secrecy is core to national security. Many government programs are shrouded in secrecy and restricted by legal classification to those with the appropriate security clearances. In nondemocratic countries, such secrecy is used to shield rulers or regimes from the scrutiny of citizens. But even democratic countries classify a growing volume of data. Among that large volume, government programs and activities in the areas bearing on information security—for example, signals intelligence, lawful interception, cryptography—are among the most highly protected.

As information control has become a top national security priority, the balance between secrecy and openness has been dramatically altered in ways that affect information security research. One noteworthy example concerns the evolving nature of computer emergency response teams (CERTs). CERTs emerged in the late 1980s as institutional responses to early Internet threats, including the Morris worm. The first CERT was housed at Carnegie Mellon University, and many that followed in the United States, Canada, and Europe were also housed within universities. Not surprisingly, they shared many of the operating principles that are associated with university culture, such as transparency, peer review, and horizontal support. When a CERT at one university discovered a worm or a bug it would typically quickly transmit that information to peer CERTs to facilitate a rapid remediation of the problem. CERTS were constituent units of what was then a self-identified community of information security peers.

Over time, however, the mission and operational practices of CERTs have evolved. Many CERTs are now situated institutionally outside universities and are formally integrated into government agencies, typically within the equivalent of public safety or homeland security departments. Many of them are staffed by former or practicing intelligence or law enforcement personnel. These changes have affected not only how individual CERTs themselves function but also the community of CERTs as a whole. For example, a research report on the evolving nature of CERTs highlighted that the influence of national security agencies on CERTs has negatively affected trust and information-sharing practices (Morgus et al. 2015). CERTs are less willing to share information in ways that they did in the past, particularly concerning software vulnerabilities. While CERTs still see themselves as part of a larger network (called FIRST), their recomposition and the influence of national security pressures have degraded the CERT regime.

## National Security Funding of Information Security Research

Pressures on the nature and type of information security research could also magnify as a consequence of strings tied to government-sponsored university-based research. National security funding can establish conditions that direct the sorts of issues that become worthy of study while deprioritizing others. Specifically, funding can close lines of communication across academic units or come with restrictions that inhibit open exchanges and circulation of ideas. The military and intelligence organs of the state have for many years financed and supported advanced research. For example, state funding of computing, mathematics, and physics was highly instrumental for nuclear weapons, ballistic missiles, signals intelligence, aeronautics, and space programs. Naturally, many of these programs were considered highly sensitive, and classification and secrecy were imposed on them and their researchers. In the 1960s, opposition to the Vietnam War in the United States generated controversy about the growing size and influence of classified university research projects, and there were substantial campus protests (Carlson 2007). Many academics expressed concerns that classified research would prevent scholars from freely disseminating their research findings, thus violating one of the fundamental tenets of academic freedom.

Since 9/11, the scope and scale of this type of sponsorship has grown substantially (Arkin and O'Brien 2015), while criticism has remained largely muted in the face of the now omnipresent justification for university research on the basis of creating jobs and deriving revenue. While some universities still have strict policies against classified research, many do not. Some, in fact, actively seek it out. Those that do seek it out find willing sponsors in national security agencies. In the United States, the National Security Agency (NSA) and the Department of Homeland Security (DHS) jointly sponsor the National Centers of Academic Excellence in Cyber Defense program, in which dozens of universities are enrolled.

As these programs grow in size and stature, a major concern is that they will begin to shape the nature of inquiry through a mix of positive and negative incentives. As the authors of a report on "the most militarized universities" in the United States note,

> The academy (and by extension the philanthropic world) has failed to establish a post-9/11 academic program to cultivate the next generation of scholars who can offer a genuinely civilian counter-narrative to the national security state similar

> to the civilian arms control community created during the Cold War. Even at the most elite schools that rank in the top 100, the many centers and research institutes focusing on warfare and terrorism are predominantly adjuncts of the national security state. (Arkin and O'Brien 2015)

Several cases illustrate how these pressures might manifest themselves. In 2013, Matthew Green, a professor specializing in cryptography at Johns Hopkins University, wrote a blog post about how the NSA had subverted encryption standards as revealed in one of the disclosures of former NSA contractor and whistleblower Edward Snowden. University administrators formally requested that Green edit his blog post by removing links to the leaked documents and the logo of the NSA. Although they later walked back their request, some believe (Anderson 2013) the impetus for it came from an individual associated with a classified research facility on campus, the Applied Physics Laboratory, which is part of the NSA/DHS centers of excellence program.

A similar case concerns a talk that was being delivered at Purdue University by the Pulitzer Prize–winning journalist Barton Gellman (2015), who was one of the journalists for whom Edward Snowden was a source. During Gellman's public talk, he included in his slides copies of the published Snowden disclosures. Afterward, Purdue University removed the video archive of the talk and went so far as to request that the projector used during the lecture be destroyed—notwithstanding the material in question being already in the public domain. Purdue University is also a participant in the NSA/DHS program, the contract for which includes strict regulations on the handling and destruction of classified material. Gellman's experience raises a broader issue of researchers' access to leaked documents housed on controversial websites like WikiLeaks.

Some government agencies specifically ask potential employees whether they have accessed classified material without permission and will not hire those who have even if the information has been published and widely read. As an author of an article advocating the use of leaked materials for academic research notes, "Researchers may encounter significant obstacles in obtaining government grants if their research relies upon information leaked from the same government" (Michael 2015).

Another illustration concerns a case in which Carnegie Mellon University researchers deanonymized users of the anonymizer tool Tor. Their presentation at a major conference was pulled however, at the request of the

Federal Bureau of Investigation, which arrested several people identified in the research. Questions were raised as to how the bureau knew of the project in advance. An answer might lie in the university's close relationship to the NSA/DHS program. Carnegie Mellon is ranked 27th among the most "militarized universities in the United States," and the Software Engineering Institute, which is where the researchers were affiliated, "was awarded $750 million in federal funding in 2015 for both classified and unclassified work" (Arkin and O'Brien 2015; see also Hern 2016).

There could be a number of other impacts of national security funding on research. In addition to stifling free expression, national security influences can affect foreign students' participation in research. A number of US schools have signed a petition (Hern 2016) arguing that US government policies restricting foreign students from being involved in sensitive research tip the balance too far in the direction of national security over academic freedom. Research that is designated by governments as classified may increase. Historically, some types of public research, such as research on diseases and weapon systems, are classified as dual use and subject to state control. Within information security, certain types of cryptography have been the subject of classification and export controls. Research into supercomputers, quantum computing, and software vulnerabilities could also face classification. As one article notes, "Tens of thousands of patent applications are manually examined each year under the Invention Secrecy Act and referred for a final decision to the Pentagon, National Security Agency, Department of Justice and, more recently, Department of Homeland Security" (Schulz 2014). With more close involvement of national security agencies in information security research, it is reasonable to conclude that classification of research could become more common.

Just as companies can attract researchers and distort the choice of topics through positive and negative incentives, national security agencies can do the same. For example, many governments are now developing very elaborate and well-resourced psychological operations that draw from psychology, sociology, and computational techniques to predict and shape behavior. One top-secret UK Government Communications Headquarters (GCHQ) document, released as part of the Snowden disclosures, "lays out the tactics the agency uses to manipulate public opinion, its scientific and psychological research into how human thinking and behavior can be influenced, and the broad range of targets that are traditionally the

province of law enforcement rather than intelligence agencies" (Greenwald and Fishman 2015). Like the NSA/DHS program, the GCHQ has sponsored cyber research centers in the United Kingdom. Cambridge University's Ross Anderson has raised concerns that programs such as these will not only steer research into topics beneficial to intelligence agencies; they will affect academic integrity. According to Anderson, "They will tell you some irrelevant and harmless top-secret fact and they will then say since this person has had access to top secret information, we need to be able to review their research for the rest of their life.… The object of the exercise is to rein in and control security research done in British universities" (Elwell 2014).

## Conclusion

As I hope to have shown, what counts as a problem worth investigating in the field of information security research is not reducible to technical or functional issues, nor does it necessarily follow an objective path based on a consensus of academics. Political and economic factors can bias those decisions and affect the nature of inquiry. Approaches to information security research that challenge the status quo or highlight nontraditional forms of information security that arguably deserve greater attention can receive less support and even strong resistance.

Mitigating the trends outlined here will not be simple, nor is there one specific solution. Instead, I propose four strategic priorities to help guide efforts into broadening, diversifying, and protecting the integrity of the field.

First, interdisciplinary approaches to information security need to be encouraged toward building a more expansive discipline of information security research that includes insights from social sciences and the humanities. Although some progress has been made in this area already, more work needs to be done. To begin, we need to remind ourselves that disciplinary silos are cultural artifacts that have their basis in particular places, times, and dominant interests. This artificial and evolving character of academic inquiry is easiest to observe when academic disciplines undergo "paradigmatic change," in the words of Thomas Kuhn (1962), or are spawned by concerted efforts. To give one example, area studies was formed during the Cold War and was spearheaded by financial support from the Ford Foundation on the basis of a perceived need to educate US policy makers about distant parts of the world (Katzenstein 2002). A similar type of field-building

exercise is required now around information security research. To be sure, field building is not a simple exercise. Quite apart from political, economic, and other factors outlined earlier, practical challenges abound. Disciplines speak different languages and are a lot like guilds in the sense of protecting their areas of inquiry from outside influence. This type of field building will require cross-disciplinary collaboration, which is time consuming, resource intensive, and organizationally difficult. The effort will require building up a community of peers to assist in review and other institutions that are essential to field building, such as peer-reviewed academic journals and premier conferences. In short, field building will take time, money, and extensive networking and advocacy. Fortunately, important seeds have been planted, in iSchools, in the subfield of security economics, and in the advances made in human computer interaction and user design to bridge engineering and the social sciences (see also chapter 6 by Hall, Madaan, and O'Hara).

Second, and relatedly, controversial methodologies that are essential to information security research will need extra protection. At a time when power is increasingly hard coded into the algorithms that surround us, academics need the ability to lift the lid and peer inside and beneath the surface (see chapter 1 by DeNardis about how "scholarship has to excavate and make visible the powers behind the curtain"). Reverse engineering in particular—a general term that covers a wide variety of tools, techniques, and methods—should be strongly entrenched as a core principle of academic freedom and an essential element of civic rights. Such protection may require adjustments to existing laws and regulations that ensure fair use for academics and shield them from frivolous lawsuits that aim to chill dissent. The Ontario, Canada, government's PPPA is one example. Another is Aaron's Law, proposed by the Electronic Frontier Foundation in 2013 as an amendment to the US Computer Fraud and Abuse Act in honor of the late computer researcher Aaron Swartz.

Third, to guard against the encroachment of national security and private sector influences that encourage secrecy and nondisclosure, information security researchers should strongly advocate for openness as a core principle of academic freedom: open access, open datasets, and open source code. Universities should, as a matter of core policy, reject research funding that places unreasonable limits on free speech and openness or induces other types of secrecy.

To be sure, governments will and should provide funding to universities for basic and applied research of all sorts as a matter of far-sighted public policy, and industry will do the same; but research should not come at the expense of bedrock principles that undergird the university system itself, such as transparency, reproducibility, publication of results, and peer review. Threats of classification loom large over information security research, particularly as governments move aggressively into developing information warfare capabilities. Writing in 2002, Eugene Skolnikoff noted that "the progress of science and technology and their unavoidable relevance to weapons conspire to enormously broaden the subjects that can be thought of as threats to security, and that expansion will continue long into the future." Information security researchers around the world will need to be prepared to face increasing encroachments on those aspects of their work whose open dissemination are deemed threats to the state.

Finally, universities should see information security not as a siloed and narrow technical discipline but as a core responsibility connected to the preservation of free inquiry and ultimately of knowledge itself. At a time when academic subjects are being narrowly justified on the basis of contributions to the economy, it is important to remind ourselves that the universities have their origin as institutions whose sole purpose was to nurture and protect knowledge for the betterment of the human condition. It was out of the university that many of the core principles of the Internet were born. Now that the Internet is under assault from forces of privatization and securitization, it is essential that academia recognize that it has not only a role to play but also a special obligation in protecting our public commons of information.

## Notes

1. I am grateful to Masashi Crete-Nishihata, Christopher Parsons, and Adam Senft for comments on a previous draft.

2. Universities are finding it increasingly difficult to retain top faculty and students in the face of the overwhelming attraction of high-salaried job opportunities in the technology sector. See *The Economist* (2016).

## References

Abbate, J. (1999). *Inventing the Internet*. Cambridge, MA: MIT Press.

Adler, E. (2008). The spread of security communities: Communities of practice, self-restraint, and NATO's post–Cold War transformation. *European Journal of International Relations, 14*(2), 195–230.

Anderson, N. (2013, September 9). Crypto prof asked to remove NSA-related blog post. *Ars Technica*. Retrieved from https://arstechnica.com/information-technology/2013/09/crypto-prof-asked-to-remove-nsa-related-blog-post/

Anderson, R. (n.d.). Economic and security resource page. Retrieved December 16, 2019, from https://www.cl.cam.ac.uk/~rja14/econsec.html

Anderson, R. (2014, May). *Privacy versus government surveillance: where network effects meet public choice* (Self-published memo). Retrieved from https://www.econinfosec.org/archive/weis2014/papers/Anderson-WEIS2014.pdf

Arkin, W. M., & O'Brien, A. (2015, November 6). The most militarized universities in America: A VICE News investigation. *VICE News*. Retrieved from https://www.vice.com/en_us/article/j59g5b/the-most-militarized-universities-in-america-a-vice-news-investigation

boyd, d., & Crawford, K. (2011, September 21). *Six provocations for big data*. Paper presented at A Decade in Internet Time: Symposium on the Dynamics of the Internet and Society. Retrieved from https://ssrn.com/abstract=1926431

Carlson, E. (2007, September 25). Scholars and secrecy—classified research comes under criticism. *NACLA*. Retrieved from https://nacla.org/article/scholars-and-secrecy-classified-research-comes-under-criticism

Citizen Lab. (2014, November). *Communities @ risk: Targeted digital threats against civil society* (Citizen Lab Report No. 48). Retrieved from https://targetedthreats.net/

Deibert, R. (2017). Cyber security. In M. D. Cavelty & T. Balzacq (Eds.), *Routledge handbook of security studies* (pp. 172–182). New York, NY: Routledge.

Deibert, R., & Crete-Nishihata, M. (2012). Global governance and the spread of cyberspace controls. *Global Governance, 18*(3), 339–361.

Elwell, M. (2014, February 14). Concern over GCHQ interference. *Varsity*. Retrieved from https://www.varsity.co.uk/news/6919

Gellman, B. (2015, October 8). Classified material in the public domain: What's a university to do? [Online forum comment]. Retrieved from https://freedom-to-tinker.com/2015/10/08/classified-material-in-the-public-domain-whats-a-university-to-do/

Greenwald, G., & Fishman, A. (2015, June 22). Controversial GCHQ unit engaged in domestic law enforcement, online propaganda, psychology research. *The Intercept*. Retrieved from https://theintercept.com/2015/06/22/controversial-gchq-unit-domestic-law-enforcement-propaganda/

Harold, S. W. (2016, August 1). The U.S.-China cyber agreement: A good first step [Blog post]. *The Rand Blog*. Retrieved from https://www.rand.org/blog/2016/08/the-us-china-cyber-agreement-a-good-first-step.html

Hern, A. (2016, February 25). US defence department funded Carnegie Mellon research to break Tor. *The Guardian*. Retrieved from https://www.theguardian.com/technology/2016/feb/25/us-defence-department-funding-carnegie-mellon-research-break-tor

Information Warfare Monitor. (2009, March 29). *Tracking GhostNet: Investigating a cyber espionage network*. Retrieved from https://citizenlab.ca/wp-content/uploads/2017/05/ghostnet.pdf

Katzenstein, P. J. (2002). Area studies, regional studies, and international relations. *Journal of East Asian Studies, 2*(1), 127–138.

Kuhn, T. (1962). *The structure of scientific revolutions*. Chicago, IL: University of Chicago Press.

Lou, E. (2015, July 30). UofT lab bane of Italian spyware firm: Leaked files. *Toronto Star*. Retrieved from https://www.thestar.com/news/gta/2015/07/30/u-of-t-lab-bane-of-italian-spyware-firm-leaked-files.html

Manovich, L. (2011). Trending: The promises and the challenges of big social data. In M. K. Gold (Ed.), *Debates in the Digital Humanities* (pp. 460–475). Minneapolis: University of Minnesota Press.

Marczak, B., Dalek, J., McKune, S., Senft, A., Scott-Railton, J., & Deibert, R. (2018, March 9). *Bad traffic: Sandvine's PacketLogic devices used to deploy government spyware in Turkey and redirect Egyptian users to affiliate ads?* (Citizen Lab Research Report no. 107). University of Toronto. Retrieved from https://citizenlab.ca/2018/03/bad-traffic-sandvines-packetlogic-devices-deploy-government-spyware-turkey-syria/

Maschmeyer, L., Deibert, R. J., & Lindsay, J. (in press). *A tale of two cyber conflicts: Civil society and commercial threat reporting*. Unpublished manuscript under review.

Michael, G. J. (2015). Who's afraid of WikiLeaks? Missed opportunities in political science research. *Review of Policy Research, 32*(2), 175–199. Retrieved from https://doi.org/10.1111/ropr.12120

Morgus, R., Skierka, I., Hohmann, M., & Maurer, T. (2015). National CSIRTs and their role in computer security incident response. *Digital Debates.org*. Retrieved from http://www.digitaldebates.org/fileadmin/media/cyber/National_CSIRTs_and_Their_Role_in_Computer_Security_Incident_Response__November_2015_--_Morgus__Skierka__Hohmann__Maurer.pdf

Pinch, T. J., & Bijker, W. E. (1993). The social construction of facts and artifacts: Or how the sociology of science and the sociology of technology might benefit each other. In W. E. Bijker, T. P. Hughes, & T. J. Pinch (Eds.), *The social construction of*

*technological systems: New directions in the sociology and history of technology* (pp. 17–50). Cambridge, MA: MIT Press.

Resnik, D. B. (2007). Neuroethics, national security and secrecy. *The American Journal of Bioethics: AJOB, 7*(5), 14–15. Retrieved from https://doi.org/10.1080/15265160701290264

Schulz, G. W. (2014). Government secrecy orders on patents have stifled more than 5,000 inventions. *WIRED*. Retrieved from https://www.wired.com/2013/04/gov-secrecy-orders-on-patents

Skolnikoff, E. (2002). Can traditional values survive? Massachusetts Institute of Technology Working Paper Series. Industrial Performance Center. Retrieved from https://ipc-dev.mit.edu/sites/default/files/2019-01/02-005.pdf

*The Economist*. (2016, April 2). Million-dollar babies. Retrieved from https://www.economist.com/business/2016/04/02/million-dollar-babies

US Department of Justice. (2014, May 19). U.S. charges five Chinese military hackers for cyber espionage against U.S. corporations and a labor organization for commercial advantage. *Justice News*. Retrieved from https://www.justice.gov/opa/pr/us-charges-five-chinese-military-hackers-cyber-espionage-against-us-corporations-and-labor

Winner, L. (1993). Upon opening the black box and finding it empty: Social constructivism and the philosophy of technology. *Science, Technology, and Human Values, 18*(3), 362–378.

Zhang, S. (2017, February 16). China's artificial-intelligence boom. *The Atlantic*. Retrieved from https://www.theatlantic.com/technology/archive/2017/02/china-artificial-intelligence/516615