Trajectories for Future Cybersecurity Research

Ronald Deibert

The Oxford Handbook of International Security
Edited by Alexandra Gheciu and William C. Wohlforth

Print Publication Date: Mar 2018
Subject: Political Science, International Relations, Political Methodology
Online Publication Date: Apr 2018 DOI: 10.1093/oxfordhb/9780198777854.013.35

Abstract and Keywords

Cybersecurity is one of the most highly contested and yet important topics. How global cyberspace is secured, by whom, and for what purpose touches upon some of the most basic of political questions. This chapter provides a survey of some of the major topics around cybersecurity and highlights some of the outstanding questions or areas for further research. The survey is not meant to be exhaustive, but rather illustrative of some of the core international political questions where evidence-based and theoretically informed social science research will be sorely needed. Cybersecurity researchers will need to explore methods that are not typically within the social science toolkit: techniques drawn from computer science, engineering, data analysis, and software development. Doing so will require bridging disciplinary divides that are not easily overcome—a challenge that may, in reality, take generations to overcome.

Keywords: cybersecurity, Internet, surveillance, Big Data, data analysis, censorship

36.1 Introduction

WHETHER it is a major corporate data breach, evidence of secret mass surveillance, or extremism on social media, nearly a day does not go by without a cybersecurity related news headline. The reasons are not surprising: human societies are going through a sea-change in communications as far-reaching as anything that has come before in modern history, but now compressed within a span of a little more than a decade. Variously referred to as “big data,” the “Internet of Things,” or just “cyberspace,” the communications environment in which we live has been vastly transformed. Cybersecurity is, therefore, a topic of obvious policy importance, but highly contested. How it is secured and by whom and for what purpose will touch upon the most basic of political questions, as infamously defined by Harold Laswell (1936): “who gets what, when, and how.”

The challenges of securing cyberspace are unique because doing so inevitably involves multiple stakeholders, including businesses, government agencies, and civil society. Since the bulk of what we call cyberspace is in the hands of the private sector, governments are compelled to enlist or otherwise compel companies in their efforts. Added to the competitive dynamic is that civil society groups and other non-state actors have been empowered by digital media, and seek to shape cyberspace to their own diverse ends, often putting them in direct competition, and in the case of militant non-state actors—*violent* confrontation, with states and the private sector.

Cybersecurity is also characterized by a unique convergence of national security and business interests around *surveillance*. For states, the threat environment has shifted over the last few decades. Whereas for most of modern history the primary security concern of most states was the threat posed by other states, today the primary threat is dispersed across all of society, inside and outside of states. On the part of businesses, the economic engine at the heart of cyberspace is the commodification of personal (p. 532) information—likes, habits, movements, relationships—acquired through acquisition of users' communications by companies such as Google and Facebook. In between the two engines of mass surveillance is a multi-billion dollar data analysis economy that services both governments and companies. This convergence of interests is where "Big Brother" meets "Big Data," creating a powerful, and very difficult-to-reverse set of forces around mass surveillance. (Lesk 2013: 86)

Because the issue is so new and dynamic, social science research on cybersecurity is still in its infancy. In this chapter, I review some of the major topics around cybersecurity and highlight some of the outstanding questions or areas for further research. This survey is not meant to be exhaustive, but rather illustrative of some of the core international political questions that require further attention from scholars.

36.2 What is Cyberspace? What is Cybersecurity?

What is "cyberspace"? The term is used widely, often undefined, or defined in many different ways, and is connected to a long history of metaphors that have their origins in science fiction (Rid 2016a: Preface). One of the widely used definitions of cyberspace, and a good starting point for historical reasons, is the one devised by the United States government. According to the "U.S. Strategic Command, The Cyber Warfare Lexicon," published in 2009, cyberspace is a "global domain within the information environment consisting of the interdependent network of information technology infrastructures, including the Internet, telecommunications networks, computer systems, and embedded processors and controllers" (US Strategic Command 2009, 8; Richelson 2016).[1]

What is notable about this definition is that it describes cyberspace as a "domain" equivalent to the domains of sea, air, land, and outer space (Kuehl 2009: 24–42). The recognition that cyberspace is a warfighting domain naturally led to the creation of the US Cyber

Command, which centralizes command of cyberspace operations across the US military. That the world's largest military defines cyberspace as a domain within which to project power, and to fight and win wars, inevitably has system-wide repercussions, both materially and ideationally. In basic terms, the reorganization of the US military prompts reorganization among allied armed forces who need to be synched up operationally in order to cooperate. Their discursive framing of cyberspace as a warfighting domain also leads to strategic and tactical explorations among theorists and practitioners, and to the development of new tools, techniques, and procedures from the defense industrial base, companies within which profit from the reorganization and new acquisition cycles. At the same time, adversaries notice the shift, the reorganization, and the build-up of forces and capabilities, and respond in ways they see fit, opening up yet more market opportunities.

(p. 533) Settling on a definition of cyberspace for operational purposes also leads to theoretical explorations of how the material properties of the "domain" differ in character from other "domains," like land, sea, air, and space. An exemplary in this respect is that put forward by Joseph Nye, who distinguishes cyberspace from other domains because it is a "man-made" environment:

> The cyber domain is a complex man-made environment. Unlike atoms, human adversaries are purposeful and intelligent. Mountains and oceans are hard to move, but portions of cyberspace can be turned on and off by throwing a switch. It is cheaper and quicker to move electrons across the globe than to move large ships long distances through the friction of salt water. (Nye 2011: 20)

Dorothy Denning, however, challenges this perspective, arguing that cyberspace is actually a mixture of natural and man-made variables, and that geography matters in cyberspace as much as in the other domains. She also takes issue with the alleged malleability of the environment, arguing that path dependencies constrain cyberspace. "While some things are easy to change in cyberspace," explains Denning, "the overall malleability of the domain is severely limited by standards, interoperability requirements, legacy software, regulations, and the resources and inertia needed to make changes" (2015: 10). Cyberspace has deep institutional and material roots that, while maybe not as fixed as a mountain, are still very formidable.

Seeing cyberspace as a single "domain" is also limited in that it masks important distinguishing features. A different way of breaking down cyberspace is the four part definition developed by David Clark. Clark (2010) defines cyberspace as the people who participate in it, the information that is stored, transmitted, and transformed within it, the logical building blocks that make it up (i.e. the software and applications), and finally the physical foundations that support the logical elements. Breaking down cyberspace in this manner allows for more specification of characteristics across the different layers of the domain. Cyberspace is better thought of as an ecosystem with multiple components that vary depending on the country and the region. In other words, there is a continuously evolving and interacting *mixture* of characteristics to cyberspace which are *contingent* on local politics, culture, geography, and technology.

There are many areas for further research related to this characterization of cyberspace, much of which requires skills that are typically not part of the toolkit of a typical social science researcher. First, mapping the infrastructure of cyberspace is an essential part of any analysis of the geopolitics of the domain in light of the fact that the infrastructure of cyberspace varies from country to country and is highly dynamic. There are numerous tools and existing data sources that can be marshalled to undertake different slices of this type of mapping. Several university-based and community-based projects exist that aim to map Internet infrastructure. The OpenNet Initiative (a project the author helped lead) undertook network measurement tests in more than 70 countries on an annual basis for several years until its cessation in 2013. A complementary project is the Open Observatory of Network Interference (OONI), "a free (p. 534) software, global observation network for detecting censorship, surveillance and traffic manipulation on the Internet." The researchers involved in this area are maturing to the point of becoming a self-identified community, including extensive discussions concerning the ethics of network measurement tests. Their research outputs have provided evidence of national Internet censorship and surveillance, and disruptions to Internet and cellphone networks around significant events, like elections or major anniversaries.

Beyond technical measurements, and recalling Clark's other layers of cyberspace, mapping should include the cultural, social, and political variables that affect cyberspace contingently. While there are similarities among countries, and significant transmission of ideas and practices from one country to another, no one country is identical to another in terms of the historical path dependencies, agencies and institutions, and unique security issues. Laws, regulations, and practices vary extensively from country to country and are important to map as part of an accurate understanding of the dynamics of cybersecurity, a challenge that requires extensive field research and understanding of local languages and cultures (Deibert et al. 2008, 2010, 2011).

36.3 Security for Whom and What?

That cyberspace does not have fixed properties across time and space, means that it is also an essentially contested space, and thus inherently political. Technologists may bristle at this suggestion, and feel that the best way to secure cyberspace would be to "leave politics out of it." But as always in life, politics—meaning the decision as to who gets what, how, and when—is inescapable. The same is no less true when it comes to cybersecurity. Regardless of whether "fixes" to cybersecurity problems are couched in techno-functional terms, cybersecurity is a contest among different worldviews, ideologies, and strategic interests even if they are obscured as unquestioned assumptions.

Myriam Dunn Cavelty has published on the social construction of cybersecurity. Drawing from securitization theory, Dunn Cavelty shows how (2013: 108) "[t]he way cyberspace is imagined and defined has consequences for the way any type of action or strategy is conceptualized." Different communities of stakeholders have differing "threat perceptions" which in turn contain different conceptual assumptions about cyberspace as a space and

place. These threat perceptions compete with each other, sometimes overlapping but other times projecting different "realms of the possible." Differing threat perceptions also delimit the range of possible policies, leaving some options out of the equation. As Dunn Cavelty (2012) explains, different ways of framing cyber threats "come with political and social effects."

Extending Dunn Cavelty's social construction of cybersecurity to the international realm, we can see how competing threat perceptions of cybersecurity manifest themselves. For liberal democratic countries, cybersecurity is primarily about protecting information networks and databases from compromise, while simultaneously freeing up information flows for the functioning of the global economy. However, as shown (p. 535) earlier, for a variety of historical and institutional reasons, military and intelligence agencies dominate cybersecurity. State-directed mass surveillance has been largely normalized and extensive resources have now been devoted to offensive cyber-espionage and warfare. The dominant position of these agencies sometimes leads to conflicts over the "referent object" of security—and whether the protection of national security should trump "network" or "user" security. A good example is the stockpiling by government agencies of computer software vulnerabilities as potential "weapons" of warfare or espionage, and the targeting of computer networks in "foreign" jurisdictions. Here, the referent object of "free, open, and secure networks" bumps up against the much more deeply entrenched paradigm of the national-security state and the defense of networks within state boundaries. Protecting "our country's" networks takes precedence over the networks of foreign countries, networks that may in fact be targeted for disruption, degradation, or even destruction.

Civil society perspectives on cybersecurity do overlap with this paradigm, but also conflict in important areas—such as around limits to mass surveillance against both government and corporations. Rather than a "domain," civil society organizations would prefer to think of cyberspace as a global *commons*—a public good—that should be shared by all, without boundaries or borders, and in which basic human rights are entrenched (Broeders 2015). Some would like to go further, drawing on theories of "liberation technology" and Internet freedom that imply cyberspace would be better off without governments altogether. But this notion seems increasingly naÏve in light of seemingly unstoppable government and corporate efforts. That said, it is noteworthy that the multi-dimensional contests between liberal democratic states, companies, and civil society means that cyberspace as it is presently constituted is subject to an informal system of mutual restraints, and a kind of "republican"-style system of checks and balances—what I have elsewhere called "distributed security" (Deibert 2012). Keeping this tug-of-war alive may be the best means to ensure Internet freedom.

Moving from liberal democratic to other countries, we see a diversification of threat models, paradigms, and stakeholder interests. China's cybersecurity paradigm, for example, while sharing some important referents with other countries around data protection, places more weight on the protection of the ruling Communist party from domestic challenges. (Lindsay 2014/15: 15–16) This attention to threats from regime challengers is op-

erationalized into extensive controls on content, downloading of policing networks to private sector service providers, and targeted digital attacks on civil society.

China also places a premium on state sovereignty in cyberspace over the multi-stakeholder model, a priority that is expressed internationally in Internet governance forums in which China increasingly participates as a major player and where it has been pushing a coalition of countries toward a common Internet governance model (Lindsay 2014/15: 37–8; Cornish 2015: 161). Whether China and other like-minded countries can succeed in promoting this agenda globally remains to be seen, but their prospects get brighter as more Internet users come from the developing world and from countries that have hybrid, mixed, or authoritarian regimes (Deibert 2015a).

(p. 536) Further research in this area could examine how threat perceptions come to be shared by different countries. Ideas, norms, and practices can be transmitted from one country to another, but the mechanisms by which they do so are unclear. Drawing from research done in other issue areas, for example environmental or trade governance, cybersecurity researchers could examine the role of norm entrepreneurs as "transmission belts," or the ways in which companies transmit practices through products and services (Deibert and Crete-Nishihata 2012). Comparative country studies on the implementation of cybersecurity policies are needed, including those that analyze new laws passed, institutions created, and practices transformed because of cybersecurity concerns (ADC and Cyber Stewards 2016).

36.4 Lifting the Lid on the Digital Environment

In spite of differing perceptions of cybersecurity, there are some inescapable trends tied to the material properties of cyberspace. One of them is the growing volume of data shared by users with third parties, and a greater number of devices connected to each other and the Internet which in turn collect, share, and transmit huge volumes of personally identifiable information. Today, we leave a digital trail wherever we go, whatever we do. How that data is protected, with whom it is shared, how it is accessed, are all important public policy and security questions.

At the most basic level, the growing number of Internet-connected devices, while convenient, presents a growing attack surface with possible cascading security consequences. Think of your Internet-enabled fridge: it allows you to remotely track the contents and see if products that are on sale at the grocery are available for purchase. But that same Internet-enabled fridge offers a potential entry point to your entire home network. If the fridge's network security is flawed, it could be the "soft underbelly" to other parts of your network. And that's just the fridge. Today there are approximately 15 billion Internet-enabled devices connected to the Internet. When we view this issue through the lens of a household, fraud, privacy violations, and theft of personal data are principal concerns. But consider the issue at a higher level: so-called "critical infrastructure," like hydroelectric dams, nuclear power plants, hospitals, or electrical grids. Cascading problems found in the software of these systems can wreak havoc on society, and even bring about signifi-

cant loss of life (Schneier 2016). Software developers do not always foresee how their systems will integrate with other systems in ways that might bring out negative externalities. Even worse is the prospect of unpatched systems "living" undetected on an ecosystem for years because the developers have stopped maintaining them. We have dramatically increased the number of digital connected devices, but the alarming number of breaches show that we have not yet figured out the security problem. As (p. 537) one author put it, "societies today network first, and ask questions later" (Eichensehr 2016: 320).

Yet another factor contributing to the security issues around our interconnected world, ironically perhaps, are actions undertaken by governments themselves in the name of national security. For example, in 2016, an unattributed group called "ShadowBrokers" released an archived repository of software exploits that they claimed were taken from the US National Security Agency's "TAO" unit. Experts who analyzed the files verified the likelihood of their source. Among the files were tools that took advantage of previously unknown vulnerabilities in a variety of widely used network routers (Biddle 2016). The revelations underscored the severity of the risks involved in network security when governments hold on to software bugs in order to use them as weapons of espionage and warfare, or to aid in law enforcement. As Schwartz and Knacke (2016: 3) say "[w]hen federal agencies discover vulnerabilities as part of carrying out law enforcement and intelligence missions, the government must determine whether knowledge of these vulnerabilities should be restricted and used for these purposes or disclosed in the national interest of improving cybersecurity." The issue underlines well the competing paradigms of cybersecurity: should the interests of national security trump user security? If so, when?

One line of evidence-based research that the Citizen Lab (a research lab at the University of Toronto, directed by the current author) has developed has been to combine technical with legal, political, and social analysis of popular instant messaging, live-streaming, and other mobile applications in order to discover hidden privacy and security risks. Several of these studies have shown that popular applications used by millions of users, most of them in China, contain hidden keyword-based censorship and surveillance functionalities presumably implemented to comply with government policies on the policing of their users. As the universe of big data progresses, this type of research will become more critical to better understanding the exercise of power "beneath the surface" of the information systems upon which we depend. Future research should explore whether applications developed in other country contexts outside of China contain similar "policing" functions.

36.5 Cybersecurity and Threats to Civil Society

As cybersecurity practices spread, governments are allocating considerable resources to new institutions (e.g. cyber commands) or to older institutions that were previously in the shadows (e.g. national security agencies). Of course the precise character of these devel-

opments vary, but one general trend is the impact of cybersecurity practices on the prospects for civil society and the flourishing of democracy.

(p. 538) Today, the fastest Internet growth rates are occurring within the world's weak, authoritarian, or mixed regimes, within countries that face governance challenges in the form of domestic insurgencies or various forms of popular discontent and digitally-empowered mass mobilization. The Arab Spring demonstrated to power elites in these countries the need to take counter-measures against groups using digital technologies. Meanwhile, state security agencies in these countries now have available to them a wide array of sophisticated products and services that allow them to undertake deep packet inspection, cellphone tracking, social media monitoring, automated trolling, and computer network attack and exploitation.

One area of concern is so-called "dual-use" technologies that provide capabilities to surveil users or to censor online information at the country network level. These technologies are referred to as "dual-use" because, depending on how they are deployed, they may serve a legitimate purpose, or, equally well, a purpose that undermines human rights. For example, certain deep packet inspection and Internet filtering technologies that private companies can use for traffic management can also be used by government-controlled Internet service providers to prevent entire populations from accessing politically sensitive information. (Dalek et al. 2016; Marquis-Boire et al. 2016) The term "dual-use" also covers malware billed as a tool for "lawful intercept," for example software exploits and remote access trojans that enable surveillance through a user's device.

It is private industry, often based in the West, that supplies much of the dual-use technology of concern (Privacy International 2016). This supply-side is now only at the very early stages of regulation and operating with little to no transparency, oversight, or accountability. Most companies in the surveillance industry have poor corporate social responsibility procedures while some have flagrantly defied such norms (Dalek et al. 2016; Dalek et al. 2015). The combination of rapid advancements in technical capabilities, lack of transparency, and the close ties of surveillance technology manufacturers with the apparatus of state security, has resulted in legal and regulatory gray areas in which companies have thus far operated with relative impunity.

Civil society organizations are bearing the brunt of this combination of forces, and are particularly vulnerable to targeted digital attacks (Deibert 2016a). Civil society organizations now depend on and have benefited from social media to conduct their campaigns and communicate with each other. Yet that same dependence on social media has become a principal point of exposure and risk, exploited by criminals, intelligence agencies, and other adversaries determined to silence dissent. Civil society is connecting at a rate that is far outpacing their capacity to secure. Many civil society organizations lack technological support, and have no means to contract with large cybersecurity firms to remediate their problems.

In the course of the last few years, research groups like the Citizen Lab have documented numerous cases of human rights defenders and other civil society actors being targeted with advanced commercial spyware (e.g. Hacking Team, Finfisher, and NSO Group) (Marczak et al. 2014; Scott-Railton et al. 2016), commercial off-the-shelf malware (in the cases of Latin America, Syria, and Iran) (Scott-Railton et al. 2014; Scott-Railton and Kleemola 2015; Scott-Railton et al. 2015), and by so-called Advanced (p. 539) Persistent Threats (APT) campaigns (in the cases of Tibetan and Hong Kong activists) (Citizen Lab 2014). Using network scanning techniques, Citizen Lab has also been able to map the proliferation of dual-use technology to a large and growing global client base, many of which are countries that have notoriously bad human rights records (Marczak et al. 2015; Deibert 2016b). Nonetheless, these findings are only touching on a small area of what is a disturbingly larger picture. The market for dual-use technologies, particularly spyware, is escalating. Government demand for these technologies may actually be increasing following the Snowden disclosures, which raised the bar on what is deemed *de rigueur* in digital surveillance (Deibert 2015a). Far from accelerating positive democratic change and liberalization, the Internet and social media may correlate with a resurgence of authoritarianism and the gradual strangling of civil society (Deibert 2015b). Unless efforts are undertaken to address in a wholesale manner the silent epidemic of targeted digital attacks on civil society, we could be facing a crisis of democracy. Further comparative research is required on how “cybersecurity” is employed to justify the implementation of policies and practices that end up furthering hybrid democracies, autocracies, and authoritarian forms of rule, and how civil society can better secure themselves from such trends.

36.6 Cybersecurity and Warfare/Armed Conflict

One important cybersecurity debate concerns the prospects of armed conflict as a result of the perceived “advantage” offense has over defense in cyberspace (Applegate 2013; Calvo 2014). It is much easier to penetrate computer networks than it is to defend them, as evidenced by the number of breaches of corporate and government networks. With the growing number of targets multiplying through the Internet of Things, and governments racing to develop capabilities to exploit those vulnerabilities (serviced by a growing market for offensive services), it seems reasonable to conclude that it is only a matter of time before a serious armed conflict erupts, either out of design or by accident (Greenberg 2015).

On the other side of the equation, however, there are those who point out the self-serving hyperbole about cyber-war (Walt 2010). Individuals associated with the defense and intelligence sectors stand to benefit by trumpeting concerns about cyber-warfare. Others express skepticism that we will ever witness a pure cyber-attack crossing the threshold to meet the Clausewitzian definition of war. The most elaborated version of this argument comes from Thomas Rid, who has pointed out there has not been a single cyber-attack resulting in loss of life. (Rid 2012) The so-called Stuxnet cyber-attack on Iranian nuclear enrichment facilities (thought to be engineered at great cost by the United States and Is-

rael), though causing considerable setbacks to the nuclear program, did not directly cause a single loss of life. Likewise, the digital attack on the Ukrainian power grid (p. 540) in 2015, largely thought to be the responsibility of a Russian state-organized cybercrime nexus, did not result in a loss of life, and power was restored with a few hours (E-ISAC 2016). As Erik Gartzke explains "[s]hutting down power grids, closing airports, or derailing communication could be tremendously costly, but most damage of this type will be fixed quickly and at comparatively modest investment of tangible resources" (2013: 57).

One of the reasons we have not yet seen, and may never see, a full-blown cyber-attack resulting in massive loss of life is that governments, even those that are adversaries, are mutually entangled in cyberspace. Insofar as we can attribute rationality to their decisions, leaders of all countries realize that attempts to disrupt cyberspace may come back to bite them, and so deterrence applies in cyberspace for the same reasons as it does with respect to deterrence in relation to kinetic attacks (Lindsay and Gartzke 2016).

While we may never see a pure cyber-war, it is important to bracket this discussion with two important caveats. First, all of armed conflict today has a some kind of digital component to it. Consider the ongoing Syrian armed conflict, where one study showed that fake female avatars on social media were used to entice opposition fighters to click on malicious links in order to get inside their computers. Using information gleaned from these computers allowed the Syrian regime to arrest and kill opposition fighters (Regalado et al. 2015). A recent Citizen Lab report showed that ISIS had used targeted digital attacks to get inside the mobile devices of opposition groups in Raqqa for the purposes of physical tracking, ostensibly for targeted murders or kidnapping (Scott-Railton et al. 2014). The same type of dynamic interplay between intelligence derived from digital technologies and their use of kinetic attacks happens on a daily basis in the War on Terror, as illustrated in targeted drone attacks (Currier and Maass 2015). So while warfare may not result solely from the use of digital "weapons," digital technologies are integral to all armed conflict today.

Second, just because it is rational for leaders to choose not to undertake cyber-attacks, the reality is that people often in engage in suboptimal or irrational behavior; accidents can happen, and misunderstandings can bring about outcomes that no one desires. Consider, in this respect, the tense situation involving China, the United States, and countries engaged in territorial disputes in the South China Seas. Should tensions emerging out of territorial disputes rise to the precipice of an armed conflict, a major cyber-related incident—like a distributed denial of service attack on critical infrastructure—could be interpreted by one of the protagonists as an "opening shot," leading to the eruption of hostilities (Libicki 2012).

In response to these contingencies, analysts and policy-makers have started to explore ways to limit warfare in cyberspace through the articulation of "rules of the road," and by elaborating on principles concerning the laws of armed conflict as they apply to cyberspace, the so-called Tallinn Manual being the most well-known of them (Meyer 2015).

These efforts are complicated by the unique properties of state competition in cyberspace, including difficulties attributing the sources of cyber-attacks, deliberate efforts to disguise the origins of operations to provide plausible deniability, the use of third-parties, or "proxies" in cyber operations, and by the blurring of cyber-espionage and -warfare. In spite of these challenges, it will be important for research to explore ways to (p. 541) limit state behavior in cyberspace to avoid armed conflict, but also to better refine ways to "verify" state and non-state behavior in cyberspace—a challenge that will require technical as well as social science methods.

One type of warfare that may become more prevalent in cyberspace is known as "hybrid warfare," which consists of the combination of subversion and propaganda with traditional strategies of kinetic warfare. One recent example of hybrid warfare is the digital infiltration of the Democratic National Committee (DNC) and other Democratic Party individuals and organizations leading up to the 2016 US Presidential election. Email accounts associated with these groups were breached and the data released to and published on Wikileaks, which led to embarrassing revelations. Forensic work undertaken by companies and security researchers, later reinforced by the US government itself, attributed the attacks to groups associated with the Russian government (Rid 2016b). The DNC episode was one example of a long-standing Russian approach to disinformation, which "consists of a deliberate disinformation campaign supported by actions of the intelligence organs designed to confuse the enemy and achieve strategic advantage at minimal cost" (Snegovaya 2015).

Hybrid warfare involving the use of social-media enabled propaganda, combined with targeted digital attacks, may be especially attractive to authoritarian regimes that are accustomed to exploiting the criminal underworld to accomplish their goals, and have few meaningful checks on clandestine activities. According to Katy Pearce, "Social media affords inexpensive and undemanding opportunities for an authoritarian regime to subtly harass opposition in front of a large domestic audience, while eschewing direct responsibility for the harassment, and measuring the spread of the harassing content" (2015: 1158). It may also be an area in which liberal democratic countries have a distinct *disadvantage*, given the role of a relatively independent and adversarial press in checking their operations.

There are many promising areas of further research around better understanding hybrid warfare. For example, Philip Howard's "Political Bots" project uses techniques from different disciplines to understand the "impact of automated scripts, commonly called bots, on social media" (Political Bots 2016). The project aims to discover how bots are used to manipulate public opinion and sow disinformation. Research that documents information disruptions around major events, such as the severing of Internet cellphone connections —what I have elsewhere called "just-in-time" blocking—offers a good complement to Howard's work (Deibert and Rohozinski 2008; Crete-Nishihata and York 2011). As in most areas of cybersecurity research, progress in this area will require the integration of tech-

nical and social science methods that are still unorthodox in the International Relations field.

36.7 Conclusion

The burgeoning universe of digital technologies and "big data" shows no signs of abating. As it continues to expand so too will the security issues that come alongside it. (p. 542) Securing cyberspace will inevitably involve highly detailed engineering and computer science techniques. But those disciplines alone can only ever provide partial answers to what are inherently political questions. The security of cyberspace is essentially contested, and is as much a struggle of power and influence as is securing other areas of life.

This chapter has provided a survey of some cybersecurity topics where evidence-based and theoretically informed social science research will be sorely needed. In order to be successful, however, researchers will need to explore methods that are not typically within the social science toolkit: techniques drawn from computer science, engineering, data analysis, and software development. Doing so will require bridging disciplinary divides that are not easily overcome—a challenge that may, in reality, take generations to overcome. Given the swift pace of change in our digital mediated world, and the enormous stakes involved for human security, one can only hope that the process of overcoming disciplinary divides can be accelerated.

References

ADC and Cyber Stewards. 2016. Surveillance and Intelligence in the Latin American Cybersecurity Agenda. *ADC Digital*, October. *Available at:* **https://adcdigital.org.ar/wp-content/uploads/2016/10/Cybersecurity-comparative-cl-ar.pdf**

Applegate, Scott D. 2013. The Dawn of Kinetic Cyber. In *2013 5th International Conference on Cyber Conflict*, edited by K. Podins, J. Stinnisen, and M. Maybaum. Tallinn, NATO CCD COE Publications, 2013. *Available at:* **https://ccdcoe.org/sites/default/files/multimedia/pdf/d2r1s4_applegate.pdf**

Biddle, Sam. 2016. The NSA Leak is Real, Snowden Documents Confirm. *The Intercept*, August 19. *Available at:* **https://theintercept.com/2016/08/19/the-nsa-was-hacked-snowden-documents-confirm/**

Broeders, Dennis. 2015. The Public Core of the Internet: An International Agenda for Internet Governance. *WRR-Policy Brief no. 2*, The Hague: WRR. *Available at:* **https://www.gccs2015.com/sites/default/files/documents/WRR%20Policy%20Brief%20(2015)%20The%20Public%20Core%20of%20the%20Internet.pd**

Calvo, Alex. 2014. Cyberwar is War: A Critique of "Hacking Can Reduce Real-World Violence." *Small Wars Journal*, April 6. *Available at:* **http://smallwarsjournal.com/jrnl/art/cyberwar-is-war**

Citizen Lab. 2014. Communities @ Risk: Targeted Digital Threats Against Civil Society. *Communities @ Risk*. *Available at:* **https://targetedthreats.net/**.

(p. 543) Clark, David. 2010. Characterizing Cyberspace: Past, Present and Future. *MIT Computer Science and Artificial Intelligence Laboratory*, March 12. *Available at:* **https://projects.csail.mit.edu/ecir/wiki/images/7/77/Clark_Characterizing_cyberspace_1-2r.pdf**

Cornish, Paul. 2015. Governing Cyberspace through Constructive Ambiguity. *Survival: Global Politics and Strategy*, 57(3): 153–76. *Available at:* **https://www.researchgate.net/publication/277134499_Governing_Cyberspace_through_Constructive_Ambiguity**

Crete-Nishihata, Masashi and Jillian C. York. 2011. Egypt's Internet Blackout: Extreme Example of Just-in-time Blocking. *OpenNet Initiative*, January 28. *Available at:* **https://opennet.net/blog/2011/01/egypt%E2%80%99s-internet-blackout-extreme-example-just-time-blocking**

Currier, Cora and Peter Maass. 2015. The Drone Papers: Firing Blind. *The Intercept*, October 15. *Available at:* **https://theintercept.com/drone-papers/firing-blind/**

Dalek, Jakub, Ronald Deibert, Sarah McKune, Phillipa Gill, and Adam Seft. 2015. Information Controls During Military Operations: The Case of Yemen during the 2015 Political and Armed Conflict. Citizen Lab, October 21. *Available at:* **https://citizenlab.org/2015/10/information-controls-military-operations-yemen/**

Dalek, Jakub, Ronald Deibert, Bill Marczak, Sarah McKune, Helmi Noman, Irene Poetranto, and Adam Senft. 2016. Tender Confirmed, Rights at Risk: Verifying Netsweeper in Bahrain. Citizen Lab, September 21. *Available at:* **https://citizenlab.org/2016/09/tender-confirmed-rights-risk-verifying-netsweeper-bahrain/**

Deibert, Ronald. 2012. Distributed Security as Cyber Strategy: Outlining a Comprehensive Approach for Canada in Cyberspace. *Canadian Defence and Foreign Affairs Institute*, August. *Available at:* **https://citizenlab.org/wp-content/uploads/2012/08/CDFAI-Distributed-Security-as-Cyber-Strategy_-outlining-a-comprehensive-approach-for-Canada-in-Cyber.pdf**

Deibert, Ron. 2015a. The Geopolitics of Cyberspace After Snowden. *Current History*, 114(768): 9–15. *Available at:* **http://www.currenthistory.com/Deibert_CurrentHistory.pdf**

Deibert, Ron. 2015b. Authoritarianism Goes Global: Cyberspace Under Siege, *Journal of Democracy*, 26(3): 64–78.

Deibert, Ron. 2016a. How Foreign Governments Spy using PowerPoint and Twitter. *The Washington Post*, August 2. *Available at:* **https://www.washingtonpost.com/posteverything/wp/2016/08/02/how-foreign-governments-spy-using-email-and-powerpoint/?utm_term=.995b323c9ced**

Deibert, Ron. 2016b. What an “MRI of the Internet” Can Reveal: Netsweeper in Bahrain. Citizen Lab, September 21. *Available at:* **https://deibert.citizenlab.org/2016/09/what-an-mri-of-the-internet-can-reveal-netsweeper-in-bahrain/**

Deibert, Ron and Masashi Crete-Nishihata. 2012. Global Governance and the Spread of Cyberspace Controls. *Global Governance*, 18(3): 339–61.

Deibert, Ronald and Rafal Rohozinski. 2008. Good for Liberty, Bad for Security? Global Civil Society and the Securitization of the Internet. In Ronald Deibert, John Palfrey, Rafal Rohozinski, and Jonathan Zittrain (eds.), *Access Denied: The Practice and Policy of Global Internet Filtering*, pp. 123–149. Cambridge, MA: MIT Press. *Available at:* **http://access.opennet.net/wp-content/uploads/2011/12/accessdenied-chapter-6.pdf**

Deibert, Ronald, John Palfrey, Rafal Rohozinski, and Jonathan Zittrain (eds.). 2008. *Access Denied: The Practice and Policy of Global Internet Filtering.* Cambridge, MA: MIT Press.

Deibert, Ronald, John Palfrey, Rafal Rohozinski, and Jonathan Zittrain (eds.). 2010. *Access Controlled: Shaping of Power, Rights, and Rule in Cyberspace.* Cambridge, MA: MIT Press.

(p. 544) Deibert, Ronald, John Palfrey, Rafal Rohozinski, and Jonathan Zittrain (eds.). 2011. *Access Contested: Security, Identity, and Resistance in Asian Cyberspace.* Cambridge, MA: MIT Press.

Denning, Dorothy E. 2015. Rethinking the Cyber Domain and Deterrence. *Joint Force* (2): 8–15. *Available at:* **http://faculty.nps.edu/dedennin/publications/Rethinking%20the%20Cyber%20Domain%20and%20Deterrence%20-%20jfq-77_8-15.pdf**

Dunn Cavelty, Myriam. 2012. The Militarisation of Cyberspace: Why Less May Be Better. In C. Czosseck, R. Ottis and K. Ziolkowski (eds.), *2012 4th International Conference on Cyber Conflict*. Tallinn: NATO CCD COE. *Available at:* **https://ccdcoe.org/publications/2012proceedings/2_6_Dunn%20Cavelty_TheMilitarisationOfCyberspace.pdf**

Dunn Cavelty, Myriam. 2013. From Cyber-Bombs to Political Fallout: Threat Representations with an Impact in the Cyber-Security Discourse. *International Studies Review*, 15(108): 105–22. *Available at:* **https://www.researchgate.net/publication/264669823_From_CyberBombs_to_Political_Fallout_Threat_Representations_with_an_Impact_Security_Discourse**

Eichensehr, Kristen E. 2016. Giving Up On Cybersecurity. *UCLA Law Review Discourse*, 64(320): 320–39. *Available at:* **http://www.uclalawreview.org/giving-up-on-cybersecurity/**

E-ISAC. 2016. Analysis of the Cyber Attack on the Ukrainian Power Grid: Defense Use Case. *SANS ICS*, March 18. *Available at:* **http://www.nerc.com/pa/CI/ESISAC/Documents/E-ISAC_SANS_Ukraine_DUC_18Mar2016.pdf**

Gartzke, Erik. 2013. The Myth of Cyberwar: Bringing War in Cyberspace Back Down to Earth. *International Security*, 38(2): 41–73.

Gartzke, Erik and Jon R. Lindsay. 2015. Weaving Tangled Webs: Offense, Defense, and Deception in Cyberspace. *Security Studies*, 24(2): 316–48. *Available at:* **http://deterrence.ucsd.edu/_files/Weaving%20Tangled%20Webs_%20Offense%20Defense%20and%20Deception%20in%20Cybe**

Greenberg, Andy. 2015. New Dark-Web Market is Selling Zero-Day Exploits to Hackers. *Wired*, April 17. *Available at:* **https://www.wired.com/2015/04/therealdeal-zero-day-exploits/**

Kopstein, Joshua. 2014. Inside Citizen Lab, the "Hacker Hothouse" Protecting you from Big Brother. *ARS Technica*, July 30. *Available at:* **http://arstechnica.com/security/2014/07/inside-citizen-lab-the-hacker-hothouse-protecting-you-from-big-brother/2/**

Kuehl, Daniel T. 2009. From Cyberspace to Cyberpower: Defining the Problem. In Franklin D. Kramer, Stuart H. Starr, and Larry K. Wentz (eds.), *Cyberpower and National Security*, pp. 24–42. Dulles: Potomac Books.

Laswell, Harold D. 1936. *Politics: Who Gets What, When, How*. New York: Whittlesey House.

Lesk, Michael. 2013. Big Data, Big Brother, Big Money. *IEEE Security & Privacy*, 11(4): 85–9. *Available at:* **http://resolver.scholarsportal.info.myaccess.library.utoronto.ca/resolve/15407993/v11i0004/85_bdbbbm.xml**

Libicki, Martin C. 2012. Crisis and Escalation in Cyberspace. *RAND: Project Air Force*. *Available at:* **https://www.rand.org/content/dam/rand/pubs/monographs/2012/RAND_MG1215.pdf**

Lindsay, Jon R. 2014/15. The Impact of China on Cybersecurity: Fiction and Friction. *International Security*, 39(3): 7–47. *Available at:* **http://www.mitpressjournals.org.myaccess.library.utoronto.ca/doi/pdf/10.1162/ISEC_a_00189**

Lindsay, Jon R. and Eric Gartzke. 2016. Cross-Domain Deterrence as a Practical Problem and a Theoretical Concept. *Cross-Domain Deterrence, UC San Diego*, July 2. *Available at:* **http://deterrence.ucsd.edu/_files/CDD_Intro_v2.pdf**

MacKinnon, Rebecca. 2012. *Consent of the Networked: The Worldwide Struggle for Internet Freedom*. New York: Basic Books. iBooks Edition.

(p. 545) Marczak, Bill and John Scott-Railton. 2016. The Million Dollar Dissident: NSO Group's iPhone Zero-Days used against a UAE Human Rights Defender. Citizen Lab and

Lookout Security, August 24. *Available at:* **https://citizenlab.org/2016/08/million-dollar-dissident-iphone-zero-day-nso-group-uae/**

Marczak, Bill, Claudio Guarnieri, Morgan Marquis-Boire, and John Scott-Railton. 2014. Hacking Team and the Targeting of Ethiopian Journalists. Citizen Lab, February 12. *Available at:* **https://citizenlab.org/2014/02/hacking-team-targeting-ethiopian-journalists/**

Marczak, Bill, John Scott-Railton, Adam Senft, Irene Poetranto, and Sarah McKune. 2015. Pay No Attention to the Server Behind the Proxy: Mapping FinFisher's Continuing Proliferation. Citizen Lab, October 15. *Available at:* **https://citizenlab.org/2015/10/mapping-finfishers-continuing-proliferation/**

Marquis-Boire, Morgan, Collin Anderson, Jakub Dalek, Sarah McKune, and John Scott-Railton. 2016. Some Devices Wander by Mistake: Planet Blue Coat Redu., Citizen Lab, July 9. *Available at:* **https://citizenlab.org/storage/bluecoat/CitLab-PlanetBlueCoatRedux-FINAL.pdf**

Meyer, Paul. 2015. Is Cyber Peace Possible? *Open Canada*, October 28. *Available at:* **https://www.opencanada.org/features/cyber-peace-possible/**

Nye Jr., Joseph S. 2011. Nuclear Lessons for Cyber Security? *Strategic Studies Quarterly*, 5(4): 18–38. *Available at:* **http://myaccess.library.utoronto.ca/login?url=http://search.proquest.com.myaccess.library.utoronto.ca/docview/1242014564?accountid=14771**

Pearce, Katy E. 2015. Democratizing kompromat: The Affordances of Social Media for State-sponsored Harassment. *Information, Communication & Society*, 18(10): 1158–74.

Political Bots. 2016. Project Description. *Available at:* **http://politicalbots.org/?page_id=129**

Privacy International. 2016. The Global Surveillance Industry. July. *Available at:* **https://privacyinternational.org/sites/default/files/global_surveillance_f.pdf**

Regalado, Daniel, Nart Villeneuve, and John Scott-Railton. 2015. Behind the Syrian Conflict's Digital Front Lines. *FireEye Threat Intelligence*, February. *Available at:* **https://www.fireeye.com/content/dam/fireeye-www/global/en/current-threats/pdfs/rpt-behind-the-syria-conflict.pdf**

Richelson, Jeffrey. 2016. The United States and Cyberspace: Military, Organization, Policies, and Activities. *National Security Archive Electronic Briefing Book No. 539*, January 20. *Available at:* **http://nsarchive.gwu.edu/NSAEBB/NSAEBB539-Declassified-Documents-on-US-Military-Activities-in-Cyberspace/**

Rid, Thomas. 2012. Cyber War Will Not Take Place. *Journal of Strategic Studies*, 35(1): 5–32.

Rid, Thomas. 2016a. *Rise of the Machines: A Cybernetic History*. New York: W.W. Norton & Company, Inc.

Rid, Thomas. 2016b. All Signs Point to Russia Being Behind the DNC Hack. *Motherboard*, July 25. *Available at:* **http://motherboard.vice.com/read/all-signs-point-to-russia-being-behind-the-dnc-hack**

Schneier, Bruce. 2016. Real-World Security and the Internet of Things. *Schneier on Security*, July 28. *Available at:* **https://www.schneier.com/blog/archives/2016/07/real-world_secu.html**

Schwartz, Ari and Rob Knacke. 2016. Government's Role in Vulnerability Disclosure: Creating a Permanent and Accountable Vulnerabilities Equity Process. *Belfer Center for Science and International Affairs*, June. *Available at:* **http://belfercenter.ksg.harvard.edu/files/vulnerability-disclosure-web-final3.pdf**

(p. 546) Scott-Railton, John and Katie Kleemola. 2015. London Calling: Two-Factor Authentication Phishing from Iran. Citizen Lab, August 27. *Available at:* **https://citizenlab.org/2015/08/iran_two_factor_phishing/**

Scott-Railton, John, Seth Hardy and Cyber Arabs. 2014. Malware Attacks Targeting Syrian ISIS Critics. Citizen Lab, December 18. *Available at:* **https://citizenlab.org/2014/12/malware-attack-targeting-syrian-isis-critics/**

Scott-Railton, John, Morgan Marquis-Boire, Claudio Guarnieri, and Marion Marschalek. 2015. Packrat: Seven Years of a South American Threat Actor. Citizen Lab, December 8. *Available at:* **https://citizenlab.org/2015/12/packrat-report/**

Scott-Railton, John, Bahr Abdul Razzak, Adam Hulcoop, Matt Brooks, and Katie Kleemola. 2016. Group5: Syria and the Iranian Connection. Citizen Lab, August 2. *Available at:* **https://citizenlab.org/2016/08/group5-syria/**

Snegovaya, Maria. 2015. Russia Report 1: Putin's Information Warfare in Ukraine. *Institute for the Study of War*, September. *Available at:* **http://understandingwar.org/sites/default/files/Russian%20Report%201%20Putin's%20Information%20Warfare%20in%20Ukraine-%20Soviet%20Origins%20of%20Russias%20Hybrid%20Warfare.pdf**

US Strategic Command. 2009. The Cyber Warfare Lexicon: A Language to Support the Development, Testing, Planning and Employment of Cyber Weapons and Other Modern Warfare Capabilities. January 5. *Available at:* **http://nsarchive.gwu.edu/dc.html?doc=2692102-Document-1**

Walt, Stephen M. 2010. Is the Cyber Threat Overblown? *Foreign Policy*, March 30. *Available at:* **http://walt.foreignpolicy.com/posts/2010/03/30/is_the_cyber_threat_overblown**

Notes:

(1.) The US military has spent enormous resources and published extensive documents on cyberspace lexicon, the volume itself an indication of the importance which the US military attaches to the domain.

Ronald Deibert

Ronald Deibert is Director of The Citizen Lab, Munk School of Global Affairs, University of Toronto.