Restrained by design: the political economy of cybersecurity

Jon Randall Lindsay

Abstract

Purpose – *The empirical record of cyberattacks features much computer crime, espionage and hacktivism, but none of the major damage feared in prevalent threat narratives. The purpose of this article is to explain the absence of serious adverse consequences to date and the durability of this trend.*

Design/methodology/approach – *This paper combines concepts from international relations theory and new institutional economics to understand cyberspace as a complex global institution with contracts embodied in both software code and human practice. Constitutive inefficiencies (market and regulatory failure) and incomplete contracts (generative features and unintended flaws) create the vulnerabilities that hackers exploit. Cyber conflict is a form of cheating within the rules, rather than an anarchic struggle, more like an intelligence-counterintelligence contest than traditional war.*

Findings – *Cyber conflict is restrained by the collective sociotechnical constitution of cyberspace, where actors must cooperate to compete. Maintenance of common protocols and open access is a condition for the possibility of attack, and successful deceptive exploitation of these connections becomes more difficult in politically sensitive situations as defense and deterrence become more feasible. The distribution of cyber conflict is, thus, bounded vertically in severity but unbounded horizontally in the potential for creative exploitation.*

Originality/value – *Cyber conflict can be understood with familiar political economic concepts applied in fresh ways. This application provides counterintuitive insights at odds with prevalent threat narratives about the likelihood and magnitude of cyber conflict. It also highlights the important advantages of strong states over the weaker non-state actors widely thought to be empowered by cyberspace.*

Keywords *International relations, Political economy, Intelligence, Conflict, Data security*

Paper type *Research paper*

Jon Randall Lindsay is Assistant Professor of Digital Media and Global Affairs at the Munk School of Global Affairs, University of Toronto, Ontario, Canada.

Introduction

President Obama wrote, "the cyber threat to our nation is one of the most serious economic and national security challenges we face [. . .]. In a future conflict, an adversary unable to match our military supremacy on the battlefield might seek to exploit our computer vulnerabilities here at home. Taking down vital banking systems could trigger a financial crisis. The lack of clean water or functioning hospitals could spark a public health emergency. And as we've seen in past blackouts, the loss of electricity can bring businesses, cities and entire regions to a standstill" (Obama, 2012). Indeed, cyber catastrophe cannot be eliminated as a technological possibility so long as every aspect of modern life depends on interconnected and reconfigurable machinery (Borg, 2005; Clarke and Knake, 2010; Kello, 2013; Peterson, 2013; Rattray, 2001; Weiss, 2010).

Yet, for a technology oft described as offense-dominant and undeterrable, there is a conspicuous historical absence of the most feared scenarios, despite epidemics of computer crime, espionage and hacktivism (Asal *et al.*, 2016; Gartzke and Lindsay, 2015; Healey, 2013; Rid, 2012; Valeriano and Maness, 2014). The cases of cyber-physical disruption that are known, furthermore, are notable for their restraint. Stuxnet did not create catastrophic failure in Iran's enrichment program, but rather aimed to slightly raise the

Received 15 May 2017
Revised 22 June 2017
Accepted 27 June 2017

centrifuge breakage rate; after an error in the code compromised the operation to the world, enrichment recovered and then increased (Lindsay, 2013; Slayton, 2017). Russian disruptions of Ukraine's electrical grid in 2015 and 2016 relied on extensive prior probing, refrained from inflicting serious damage and were mitigated within hours (Zetter, 2016; Cherepanov, 2017). Russian influence operations targeting the 2016 US election unfolded over many months with at best ambiguous effectiveness (Sanger *et al.*, 2016; Rovner *et al.*, 2017). Meanwhile, despite the steady drumbeat of threat rhetoric, firms and utilities around the world continue to invest more of their value into digital networks. Either they negligently tempt fate or the profitability of interconnection exceeds their perception of the risk (Lindsay and Cheung, 2015).

What explains the absence of serious consequences to date and how durable is this trend? Perhaps, we have simply been lucky that widespread complacency has not yet been punished. Another possibility is that weaponizing cyberspace may be beyond the capacity of many terrorists or even state actors (Benson, 2014; Buchanan, 2017; Herrick and Herr, 2016; Slayton, 2017). Those actors who can overcome the barriers to entry may lack the motivation to inflict harm via surprise attack, or they may be deterred by the prospect of military or economic retaliation (Gartzke, 2013; Libicki, 2009; Liff, 2012; Lindsay, 2015; Lindsay and Gartzke, 2017). At the same time, many government agencies and defense firms have a political or financial interest in peddling exaggerated narratives of cyber doom (Lawson, 2013; Brito and Watkins, 2011; Dunn Cavelty, 2008). These complementary explanations are empirically supported (Healey, 2013; Valeriano and Maness, 2015), but perhaps future conditions will change. Costs could decline and interests could change, making destructive hacking attractive and vindicating alarmists. I argue deductively, however, that restraint in cyberspace is not just an historical accident. On the contrary, incentives for moderation are built into its cooperatively constructed infrastructure, and these incentives grow stronger as more economic and administrative functionality moves online[1].

"Cyberspace" shares its Greek root with "government" and should be understood accordingly as not just an engineering artifact but, quite literally, as "control space" that extends governance via technical means (Beniger, 1986; Kline, 2015; Rid, 2016). People adopt information technology to reduce the transaction costs of measurement, coordination and enforcement, thereby enhancing control over organized behavior. Not only does cyberspace have institutions like internet firms and the Internet Corporation for Assigned Names and Numbers (ICANN), but also, in a much more fundamental sense, cyberspace is an institution. One implication is we can make sense of this sprawling sociotechnical assemblage with familiar political economic concepts; cf. (Choucri, 2012; Eriksson and Giacomello, 2006; Kello, 2013). Another is that, to the extent that institutions create disincentives for conflict in international relations, we should expect the stakeholders in a complex sociotechnical system to refrain from inflicting great harm on one another.

The relationship between institutions and war is, of course, one of the most enduring and controversial topics in international relations (Carr, 1939; Deudney, 2007; Keohane, 1986; Keohane and Martin, 1995; Mearsheimer, 1994). The traditional debate asks whether normative laws and values can restrain military power and physical violence. Yet, in the case of cyberspace, the substantive difference between the means of restraint and the means of aggression diminishes. Participation in the institution is the condition for the possibility of conflict within it, and this makes all the difference. Actors adopt common technical standards and protocols to maintain the connections they need to engage in beneficial exchange or deceptive exploitation, but voluntary connections can be withdrawn. Cyber operations work by cheating at the margins of the cooperative agreements that make cyberspace work, not by breaking them altogether, as happens in confrontational warfare. Of course, states can always resort to violence as the ultimate arbiter of disagreement, and cyber operations can, indeed, support the use of force by military means, for example, by shutting down enemy air defenses to create a window for

air strikes. Cross-domain scenarios create some danger of inadvertent escalation due to miscalculation and pressures to act fast arising from cyber capabilities (Cimbala, 2012; Gartzke and Lindsay, 2017; Gompert and Libicki, 2014; Libicki, 2012). Yet, incentives for restraint *within* the cyber domain exist even in war because the tactical coup relies on implicit agreement by the enemy to leave its systems open. Surprise attack, or careless tradecraft in the preparation for it, encourages the enemy to reconfigure its networks, which, in turn, undermines the possibility of future deception. Preserving maneuver room for cyber exploitation is, ironically, a cooperative endeavor.

Cybersecurity is preoccupied with inefficiencies and adaptation within a shared global institution rather than existential contests between dueling hierarchies in anarchy. I do not take a strong position here on whether cyberspace, as an institution, enables actors to exit from anarchy. Certainly, information technology reinforces other liberal institutions and enhances the value and efficiency of global trade, so it very well may be an intervening variable in prominent explanations for peace (Ikenberry, 2001; Gartzke, 2007; Keohane and Nye, 2001). Greater levels of cooperation in the construction of mutually valuable infrastructure tend, over time, to extend the scope and scale of sociotechnical control for all stakeholders. As the incidence and intensity of actual warfare declines historically, for whatever reason (Mueller, 2004; Gat, 2006; Pinker, 2011; Morris, 2014), virtual conflict becomes more attractive.

This article proceeds in four parts. First, I develop the notion of cyberspace as a sociotechnical institution. Second, I show how constitutive inefficiency creates exploitable vulnerabilities in it. Third, I argue that cheating is self-limiting for coercion or revision in cyberspace. I conclude by arguing that improvements in cybersecurity will tend to encourage more devious, but less damaging attacks in the future.

Cyberspace as an institution

In the paradigm of new institutional economics (North, 1990; Ostrom, 1990; Stiglitz, 2002; Williamson, 1981), "Information processing by the actors as a result of the costliness of transacting underlies the formation of institutions" (North, 1990, p. 107). We should, thus, expect devices designed expressly for improving information processing to have a particularly institutional character. Historically, there has been a close co-evolution between information technologies and social institutions to improve people's ability to measure behavior and resources, coordinate collective action and enforce their intentions (Beniger, 1986; Crosby, 1997; Scott, 1998). The vernacular of computer science abounds with bureaucratic nomenclature (code, procedures, routines, programs, protocols, files, folders, registries, etc.), and a key intellectual insight of the cybernetics movement was that feedback machines worked like governors, both the automated and political kinds (Agar, 2003; Deutsch, 1963; Dupuy, 2000; Medina, 2011).

If institutions are "the rules of the game" (North, 1990, p. 3), then technology is the playing equipment and the field on which the game is played. Indeterminate on their own, human-built normative and material constraints (i.e. rules and tools) work together to make transacting more reliable. Speed limits can be enforced by policemen or speed bumps (Lessig, 2006, 127-28). Conversely, athletes can cheat by either fooling referees or modifying game equipment. Politicians create bureaucracies to lock in favored policies beyond their incumbencies (Moe, 1990). By a similar logic, "software is frozen organizational and policy discourse" (Bowker and Star, 1999, p. 135) which gives inertia to the resolution of controversies (Latour, 1987; Mackenzie, 1990; Winner, 1980). Software tools are literally built out of rules.

Cyberspace is not anarchy

Cyberspace is typically mistaken for an ungoverned anarchy, the very opposite of an institution. In 1997, the head of Google described the internet as "the largest experiment in anarchy that we have ever had" (Schmidt and Cohen, 2013, p. 222). Analysts with an

American think-tank write, "The cyber commons today is a complex and anarchic environment lacking effective international agreements [. . .]. Users – whether organizations or individuals – must typically provide for their own security" (Rattray *et al.*, 2010, pp. 148-149). According to General Hayden (2016), "the cyber domain had never been a digital Eden. It was always Mogadishu". Scholars at the US Naval War College argue that states are only now beginning to tame this anarchic frontier (Demchak and Dombrowski, 2011, p. 32).

However, the internet is emphatically not anarchy in the sense in which the term is used in international relations theory. According to a prominent realist theorist, institutions are distinguished from anarchy by "the differentiation of units and the specification of their functions" (Waltz, 1979, p. 88). In anarchy, an actor "decides for itself how it will cope with its internal and external problems, including whether or not to seek assistance from others and in doing so to limit its freedom by making commitments to them" (Waltz, 1979, 96)[2]. Anarchy incentivizes self-help because autonomous states cannot rely on a higher authority to enforce contracts and other states might attempt to renegotiate with force (Fearon, 1995; Glaser, 2010; Jervis, 1978; Wagner, 2000).

Cyberspace might even be described as the largest experiment in institutions ever. By improving the efficiency of global economic exchange (Brynjolfsson and Saunders, 2010; Starrs, 2013) and facilitating civil society discourse, the internet reinforces the state-guided but decentralized liberal order that the USA built after the Second World War (Drezner, 2004; Ikenberry, 2009) – a conflict better described as the greatest experiment in anarchy ever. Cyberspace protocols are decentralized and its operation is massively distributed, to be sure, but this network of networks is a densely institutionalized sociotechnical system that improves the efficiency of economic transactions and supports unprecedented specialization. Hardly a self-help system, internet actors let others help them in almost everything they do. Users rely on software vendors, public utilities, banks, insurance firms, law enforcement and government regulators to protect their data and ensure the reliability of their online experience. All of these actors, in turn, rely on the predictability of other actors in a system that they cannot possibly understand in detail, which enables them to ignore security most of the time.

Constitutive contracts

Cyberspace can be conceived in political economic terms as an assemblage of overlapping regulatory mechanisms and negotiated contracts implemented by both people and machines. Software is a system of rules that can be likened to contracts in deterministic code, rather than just interpretable human language, because they constrain the runtime behavior of machines and set expectations for other actors. This is not a huge conceptual leap, given that the cybernetic tradition gave rise to game theory, which informs economics, and information theory, which informs computer science (Kline, 2015; von Neumann and Morgenstern, 1944). General purpose computers implement logical sets of instructions, which are be combined into higher-order languages like C++ to write operating systems like Linux, libraries of common functions, and applications like PowerPoint, which are flexible enough to support a church group or a military battalion. A hierarchy of technical protocols enables a limitless variety of software applications to interface with a limitless variety of hardware devices circuits via Transmission Control Protocol/Internet Protocol (TCP/IP). Virtualization enables programs to call software services without knowing where server hardware actually resides, and service providers can swap out machines and balance loads without disrupting the running programs. Abstractions like the software stack, internet hourglass and cloud computing enable vendors, administrators and users to focus on just a particular task, insulating themselves from other activities (and errors) above or below them in the system of abstraction. These

layers nest like a Russian doll, and there seems to be no upper bound on the art of abstraction.

From the point of view of the abstraction developer, who is concerned with the reliability of the software construct, code that explicitly handles every possible combination of input conditions provides a complete contract within the scope of the abstraction. Mathematical proof is the best certification of the completeness of an algorithmic contract. In practice, formal proofs are infeasible for complex applications, and developers inevitably make mistakes. Bugs are, essentially, unintentionally incomplete contracts. Bugs can cause programs to crash, compromise data integrity or otherwise violate a programmer's expectations when the deterministic machine encounters conditions not precisely specified in the software contract. Many developers aspire to create software that fails gracefully, via error detection and correction logic to mitigate the effects of a broken contract. However, the higher-order enforcement contracts that they write may have bugs as well. From the point of view of the application developer, who is concerned with meaningful human-computer interaction, a software abstraction is an intentionally incomplete contract that is flexible enough to deal with a wide range of unforeseeable situations. Abstract features enable developers to code software contacts that link different users and use cases by leveraging many simpler contracts that other developers have written and debugged in advance. A developer who writes a library routine does not have to anticipate everything that third-party developers will want to do with it, and an end user does not have to rewrite a basic function every time she/he wants to calculate something. Modularity is generative (Baldwin and Clark, 2000).

Hackers exploit both features and bugs as they work within the letter of the law but violate its spirit, as discussed in the next section. Modern computing systems work through trillions of interlocking incomplete contracts that have been negotiated in advance by designers and developers widely distributed in space, time and national origin. Internal code reviews by vendor firms, bug reports from customers and the inspection of open-source software by distributed communities enable developers to debug – or renegotiate – inefficient software contracts. Hierarchies of software abstraction have, like any other institution, evolved along a historically contingent path shaped by distributed negotiation, which can sometimes lock in inefficient or outdated contracts, hence the glacial pace of transition from IPv4 to IPv6 (DeNardis, 2009). Developers have to trust the benign intentions, technical skills, and quality control processes that enable the specification of contracts that they do not have the time or ability to inspect. The entire software fabric of cyberspace is, thus, a network of deals, most of them cooperatively specified in good faith. Malicious exploitation abuses this trust by using the same generative computing tools that enable productive applications to code malware and play confidence games with users (Zittrain, 2006). A more complex institution relies on more complex trust relationships, which creates more potential for complex cheating.

The human scaffolding of cyberspace is at least as sophisticated as the network of automated contracts. Some groups are loosely coordinated, others closely regulated; some share openly, others are more secretive; some provide public goods, others buy and sell private goods (Benkler, 2006; Hess and Ostrom, 2007; Hurwitz, 2012; Messerschmitt and Szyperski, 2003; Rosenzweig, 2013). The majority of design and day-to-day administrative decisions falls to non-state actors and decentralized transactions. Internet service providers, for example, cooperate through close-knit Network Operators Groups to route traffic efficiently and limit abuse, such as spam and service denial attacks, providing the common resources of bandwidth and efficient addressing on which all public and private uses of the internet depend (Sowell, 2015). The constant adjustment and repair of constitutive rules and tools is all but invisible to most users (Downey, 2001). Commercial hardware and software vendors create the majority of devices that implement cyberspace, but academic scientists, government labs and private citizens also make important

contributions through open institutions like the Internet Engineering Task Force and Internet Society. Some parts of the internet, like the Domain Name System coordinated by ICANN, are explicitly hierarchical and attract considerable governmental attention. Utopian dreams of some internet pioneers notwithstanding, national governments have proved willing and able to enforce domestic laws to remove offensive content, arrest hackers, regulate businesses and shape technical architecture in their territory (DeNardis, 2014; Goldsmith and Wu, 2006; Mueller, 2010).

Cyberspace is an institution, firstly, because information technology supports fundamental institutional functions of measurement, coordination and enforcement, and secondly, because the internet relies on unprecedented specialization and cooperative interdependence to implement these functions at scale. Cyberspace is literally constructed out of a web of contracts or mutual constraints implemented in software, legal documents and human habits. The negotiation and renegotiation of its constitutive contracts are coordinated through both centralized governance and decentralized institutions that co-evolve with its centralized and decentralized technical architectures. This system of mutually constitutive normative and material processes is not a rigid hierarchy, clearly, but it has far too much specialization and interdependence to be considered truly anarchic. Unsurprisingly, the sociotechnical complexity in this massively distributed institution generates a lot of data friction across it many overlapping surfaces (P. N. Edwards, 2010). Constitutive inefficiency, in turn, creates the vulnerabilities that hackers exploit.

Hacking a sociotechnical institution

Hackers can only move through doors accidentally left open or unwittingly opened for them. Because code is mere logic, it cannot use brute force to break down doors. "There is no forced entry in cyberspace" (Libicki, 2007, p. 31). If a door is closed by a software patch, a changed configuration setting, or user vigilance, then no amount of typing will pry it open. The complete substitution of information for mass in cyberwarfare entails total reliance on stratagem instead of material power. If cyberspace is an institution, then cyberattack is a form of cheating within it. Cheating within the rules is like speeding up at a yellow light: the warning is intended to slow cars down to improve safety, but driving through the intersection is still legally permitted, even as it degrades safety. Cyberattacks, likewise, play within the rules but achieve unintended results. They are inherently deceptive because they instruct perfectly obedient (i.e., deterministic) machines to behave in ways that are harmful to people who trust them to behave helpfully.

Cheating within the rules

Vulnerabilities are the result of incomplete contracts. Developers who code incomplete contracts, either intentionally as features or unintentionally as flaws, become unwitting parties to their own exploitation, which is the essence of deception. Malware leverages prepackaged computer functionality to turn on cameras and microphones, log keystrokes and screenshots, gather data for covert exfiltration or send commands to other trusted machines and hardware peripherals on a private network. Espionage networks can use social media accounts or webmail inboxes to pass commands back and forth to infected hosts, masquerading as legitimate users (Adair *et al.*, 2010; FireEye Threat Intelligence, 2015). Because general purpose computers store instructions and data in the same memory space, techniques such as buffer overflow attack, SQL injection and cross-site scripting can smuggle instructions from the data stream into the execution flow to hijack control of the machine. These hacks work with depressing frequency because ignorant or complacent developers fail to write error-checking code. The best technical tricks exploit flaws that vendors have not discovered or patched. So-called zero days are like open doors that the vendor does not know it should lock (Leyla and Tudor, 2012; Zetter, 2015). All of these vulnerabilities lurk in the excess informational variety that is present in the environment but which the deterministic target system fails to handle properly.

Social engineering attacks deceive human users to get around technical defenses. An attacker might impersonate an official from the ISP or the government to ask users to reveal their password. Watering hole attacks impersonate popular websites to fool visitors into clicking on unsafe links. Spear phishing attacks use emails crafted to appear like they are from a trusted colleague or family member to fool the recipient into opening an infected file, in some cases, defeating two-factor authentication schemes (Railton and Kleemola, 2015; Scott-Railton *et al.*, 2015). Supply chain attacks replace hardware with tampered devices for the purposes of espionage or sabotage (Weiss, 1996). The Equation malware, allegedly written by the American NSA, was distributed via infected CD-ROMs to foreign participants in a scientific conference in Houston (Global Research and Analysis Team, 2015). The Buckshot Yankee infection of US military classified computers appears to have originated with an infected USB key provided by a Russian intelligence service to an unwitting mule on an American base overseas (Grindal, 2013). All social engineering techniques rely on fraud, duplicity and confidence games. They create more relevant variation in the world than the sociotechnical target is able to detect and mitigate.

Institutional vulnerabilities

Why do not vendors, network operators and users just repair or modify technology to make it harder for malicious actors to repurpose it in the first place? Unfortunately, the actors who can make cyberspace more secure are often not motivated to do so, while other actors exploit public goods for private gain (Anderson and Moore, 2006; Bauer and van Eeten, 2009).

The sheer complexity of software systems creates serious coordination problems (Brooks and Frederick, 1995). Public goods with concentrated costs and diffuse benefits tend to be underprovided (Olson, 1965). Security engineering is expensive because vendors must methodically review code and exhaustively test for flaws. Some flaws can hide in plain sight for years, such as the Heartbleed bug in the OpenSSL implementation of TLS (Durumeric *et al.*, 2014). Nonobvious security risks are then borne by third-party users when downstream developers recycle buggy components. For example, Baidu Browser was found to have serious privacy flaws that transmitted detailed user information in the clear or via easily decryptable encryption, enabling an attacker to inject arbitrary code onto a mobile device; moreover, the leaky Baidu software development kit (SDK) used by hundreds of applications available from Google Play exposed users to the same privacy and security risks (Knockel *et al.*, 2016). Software coordination problems, thus, tend to exacerbate information asymmetries and negative externalities.

Software security is notoriously hard to measure, and if consumers cannot tell which software products are more or less secure, then they will be less likely to pay the higher premium to venders who make security investments. Fake antivirus scams promise to protect computers but actually infect them. Temptingly free games, movies and music become a vector for infection. A Chinese version of the Skype platform installs spyware for government censors (Markoff, 2008). One remedy in a market for lemons is for a reputable third party to certify the quality of goods (Akerlof, 1970), e.g. ownership history reports on user. Unfortunately, certifications can be abused. One study found that the websites certified as safe by TRUSTe were more than twice as likely to be risky compared to uncertified websites (Edelman, 2011). Attackers who forge or steal cryptographic certificates or otherwise subvert a certificate authority (CA) can install malware masquerading as CA-approved software, a technique leveraged by Stuxnet and the attack that bankrupted a Dutch CA (Hallam-Baker, 2013).

The profitability of many information technologies is a function of positive network effects (Shapiro and Varian, 1999). A phone becomes more useful when there are more people to call, and an operating system is more useful when there are more applications written for it. Unfortunately, increasing returns incentivize vendors to rush functionality to market

without building in security, which takes more effort and may even complicate the functionality of the product. When a firm ships software with a security vulnerability, then every instance of that software on the market will have it. Consumers, in turn, are often willing to use insecure software or forego patching because they do not personally bear the costs (August and Tunca, 2006). One infected host in a botnet may suffer negligible performance degradation, but third parties attacked by the botnet may lose valuable intellectual property or suffer service denial. Similarly, a factory or public utility may connect machinery to the internet for the convenience of remote monitoring and upgrading, but this exposes critical infrastructure and downstream users to the risk of cyber-physical attack. Many factories do not apply the most up-to-date security patches or they rely on unsupported versions of operating systems because they worry that upgrades would disrupt industrial operations (Nelson, 2016). Network effects can also lock in inefficient software or protocols that contain vulnerabilities. The adoption of a more secure DNS protocol has been similarly impeded by high switching costs and widespread commitment to the earlier and less secure protocol.

The usual remedy for market failure is government regulation, but policy can introduce additional vulnerabilities. Government-mandated backdoors intended to improve law enforcement surveillance and thus public security have the perverse effect of creating vulnerabilities that can be exploited by criminal and nation state hackers (Landau, 2010; Abelson *et al.*, 2015). The imposition of mandatory standards by government regulators or corporate administrators can inadvertently weaken security or performance by slowing adoption of more efficient products and practices introduced in the market (Claffy and Clark, 2014). Vendors have begun to take a more active interest in engineering security because of growing public worries about privacy and the marketing efforts of a growing cybersecurity industry, which militates against some of the externality and coordination problems mentioned above. Some critical internet resources such as bandwidth and ISP interconnectivity are provided through the spontaneous coordination of technical operators who share an interest in maintaining the quality of the technical playing field, even though they are used by competing firms. The Conficker epidemic, for example, was mitigated through decentralized coordination, rather than government intervention, which, counterfactually, might have slowed the response (Bowden, 2011). Another perverse result of government security efforts is that offensive stockpiles of so-called zero-day vulnerabilities can impede vendor efforts to patch for the common defense: offensive potential depends on not revealing the flaw to defenses used by enemy and friendly computers (Zetter, 2015).

Yet, even if the market does provide effective security features, they are useless if myopic routines and principal-agent problems keep bureaucracies from using them. The sources of vulnerability and security in cyberspace are found in the tradeoffs between centralized and decentralized, or government and market, modes of organization. These are basic tradeoffs in any institution, but they are especially complicated in a layered, global, decentralized control system.

Institutional limits on cheating

Cyberspace creates many new opportunities to deceive developers and users, but effective deception can be difficult and hackers can be deceived; after all, hackers are developers and users, too. Deception becomes a liability when compromise is dangerous, and a deception is harder to maintain in complex situations. Moreover, the defender can use deception as well through active monitoring, investigation and hunting techniques (Bejtlich, 2013; Bodmer *et al.*, 2012; Gartzke and Lindsay, 2015). The costs of deception may outweigh the benefits against some targets. Reliance on deception also complicates political objectives that depend on credibly conveying information to an adversary.

The limits of coercion

Coercion concerns the power to hurt in the future, not the brute force of hurting now (Schelling, 2008). An aerial bombing campaign may reduce the target's material capability, for example, but it may also demonstrate an ability to cause even greater reduction of capability and loss of value in the future. The historical record of strategic bombing as a coercive instrument, however, especially when used without complementary ground forces, is rather dismal (Pape, 1996; Biddle, 2002; Haun, 2015). It is unlikely that nonlethal strategic bombing would fare much better[3]. The unsuitability of cyberwarfare for coercion is even more fundamental because it relies on deception. The classic diplomatic signal of resolve in a crisis is the mobilization of the army to deter an attack. Mobilization is costly regardless of whether war breaks out, and it improves performance in war, in case war does break out, which convincingly separates resolved states from bluffers (Slantchev, 2011). By contrast, threatening a specific surprise attack alerts the target to close the vulnerabilities upon which the attack relies and provides the victim with a target for retaliation. An ambiguous threat that does not reveal the actual vulnerability is less credible for distinguishing a genuine signal from a bluff (Gartzke, 2013; Lindsay, 2015; Lindsay and Gartzke, 2017).

The first major attempt at cyber coercion was the 2007 distributed denial-of-service (DDoS) attacks against Estonia (Schmidt, 2013). The removal of a Stalinist statue sparked street protests and DDoS attacks against government and financial websites. The attacks were quickly mitigated through the informal collaboration of the Estonian technology community, but they persisted in some form for two-and-a-half weeks without anyone issuing any demands. Estonian banks suffered real financial costs, but Estonia did not replace the statue, and Tallinn became more resolved to cooperate with the West. Indeed, Estonia has become the hub for coordinating NATO cyber defenses. Ambiguity about responsibility persists, with some evidence suggesting the Russian government in collaboration with so-called patriotic hackers. The Estonian attacks, like most DDoS episodes, amounted to an ambiguous symbolic protest with little coercive leverage for Russia. Anonymous outbursts may tell you that someone is upset, but they also tell you that someone is not upset or confident enough to really do something about it.

The hack of Sony Pictures Entertainment in late 2014 further demonstrates how attackers who depend on anonymity become vulnerable when they lose it (Haggard and Lindsay, 2015). Hackers calling themselves "Guardians of Peace" defaced Sony computer desktops, wiped corporate hard drives, released embarrassing internal documents, demanded that Sony not release *The Interview* (a raunchy satire about the assassination of Kim Jong Un) and ominously warned, "Remember the 11th of September 2011". The threat of terrorism, however implausible, pushed movie theaters and Sony to cancel the release, but it also put pressure on the US government to respond. In an unprecedented attribution of a foreign government, President Obama explicitly blamed North Korea. The hackers stood down immediately, Sony decided to go ahead with *The Interview*, and Obama levied sanctions against three organizations and 10 officials in North Korea. Notably, the attacker felt the need to anonymously threaten something other than cyberattack to inspire fear (terrorism), and the USA chose a punishment other than cyberattack for its deterrent response (sanctions). The attack cost Sony a mere US$15m and the resignation of its co-chairman, who promptly started a new production company (Rushe, 2015; Faughnder, 2015). North Korea not only failed to prevent release of *The Interview* but probably encouraged many more people to watch the poorly reviewed movie than would have otherwise.

Cyberwarfare is a poor instrument for signaling because deception revealed is deception defeated. This problem encourages pessimism about the use of cyber threats alone for deterrence (Elliott, 2011; Lupovici, 2014). A demonstrated capacity for sophisticated operations and a stockpile of zero days, as the Snowden leaks credibly signaled for the

NSA, may enhance general deterrence (which dissuades challengers), but is of less utility for immediate deterrence (which persuades challengers to back down). Fortunately, unsuitability for deterrence (coercion to prevent action) is also unsuitability for compellence (coercion to compel action). Ambiguous signals with unclear costs are hard to distinguish from the noise, and it is difficult for the target to determine what actions, if any, might suspend the punishment. This is one reason, beyond the significant technical difficulties of weaponizing physically destructive cyberattacks discussed below, why terrorists find guns and bombs more reliable instruments of intimidation (Benson, 2014). Deception is ill-suited for credible communication, but it has other advantages. This is why a predator ambushes its prey without warning because it wants something to eat.

The limits of revision

Asset theft, clandestine intelligence collection, covert influence and surprise attack aim to marginally revise the distribution of power between competing actors. Deceptive revision exploits the willing cooperation of the target rather than seek out direct confrontation. Yet, cheaters have to avoid getting caught and avoid being cheated themselves. An attacker has to be able to plan and execute the attack and take advantage of the effects it creates, but the challenges increase with the complexity of the operation and value of the target.

Table I highlights the variation in the costs and risks across three different types of cyber operations. This is a coarse parse intended to illustrate variation. I do not, for instance, break out hacktivism that uses defacement, doxing or DDoS as a form of political protest as a separate form of crime or intelligence. Russian "active measures" used during the 2016 US election combined espionage tradecraft and influence techniques and mobilized decades of intelligence experience. Each of the three types of operation described here has some expected benefit and a number of associated costs. These include the

Table I Characteristics of cyberattacks

	Crime	*Intelligence*	*Warfare*
Utility of deception	Monetary gain	Intelligence advantage	Tactical surprise or chronic friction
Access	Any exposed or gullible target on the internet	A specific target and data protected by network defenses	Same as espionage plus access to industrial control system or military C4ISR
Vulnerability	Known vulnerabilities in complacent targets	Combine multiple vulnerabilities and zero days	Same as espionage plus vulnerabilities in specific controls and machinery
Payload	Infect host or steal accounts and credentials	Exfiltrate target data to own C2 network	Predictably alter performance or cause malfunction in critical infrastructure
Follow-through	Monetize or launder illicit data	Disseminate recovered data to someone who can understand and use it for political or economic advantage	Political/military exploitation of the temporary window of opportunity created by the attack plus damage assessment
Consequence of compromise	Move on to the next mark, risk of law enforcement response	Lost access, burned vulnerabilities, risk of counterintelligence entrapment	Same as espionage plus missions that depend on the attack may fail, plus risk of cross domain retaliation
Organizational capacity	Low barriers to entry for individuals	Small team with technical expertise and planning ability	Well-resourced, experienced, compartmented teams able to solve difficult planning, testing and execution problems that require multiple categories of expertise and expense in extreme secrecy
Frequency	Prevalent	Intermittent	Rare

operational challenges of gaining access, exploiting vulnerabilities and controlling payloads. Attacker mistakes or defensive efforts in any of these areas may not only cause the attack to malfunction but also leave clues that can compromise the operation and prompt retaliation (B. Edwards *et al.*, 2017; Rid and Buchanan, 2015). Even if the attacker is able to pull off a successful deception, additional follow-through is needed to convert the intrusion into a political or economic benefit. Costs and risks mount with more ambitious attacks because target complexity increases the chance of malware malfunction and compromise, while target value increases the defensive effort invested in network protection and intrusion response (Lindsay, 2015). Attacker risk will mount considerably as defenders use counterintelligence and active defense techniques (Bodmer *et al.*, 2012; Bejtlich, 2013). Mounting challenges necessitate greater organizational capacity for planning the operation, tailoring malware access and payload to target vulnerabilities, rehearsing the operation, conducting surveillance detection, maintaining operational security discipline and dealing with the consequences of failure or retaliation, should either occur. As a result, low risk but low-impact cybercrime is prevalent; high risk but potentially high-impact cyberwarfare is rare; targeted espionage falls somewhere in between.

Cybercrime for theft, fraud and illicit advertising is usually untargeted and fails more often than it works. Yet, cybercrime can fail most of the time and still be profitable in the aggregate. Just as a petty burglar rattles door handles until one opens, most criminal malware uses the internet for indiscriminate access and exploits known vulnerabilities that complacent targets leave unguarded. Target-agnostic cybercrime is scale-independent, so there is little cost associated with trying millions of doors (Herley, 2013). Even when doors do open, stolen bank accounts have no value if the thief cannot spend the funds or suspicious banks are willing to block accounts and roll back transactions. The largest obstacle to profit is the monetization of ill-gotten gains, requiring criminals to devise money laundering schemes through merchandise resale or mules who withdraw small deposits (Hao *et al.*, 2015). While the barriers to entry for cybercrime may be as low as an internet connection, most participants in the underground economy do not make that much money because of ruthless competition, value-eroding specialization and the risk of being cheated by other criminals (Herley and Florêncio, 2010; Molnar *et al.*, 2010).

By contrast with wholesale cybercrime, an advanced persistent threat (APT) targets specific organizations or information. APTs require better intelligence, more skill and some patience to hack the specific characteristics of the target, find what they are looking for and exfiltrate it back through their C2 network. Attackers can try known vulnerabilities in hopes that a target is complacent, but for vigilant defenders with updated patches, zero days are helpful. The use of multiple zero days in a single intrusion is often the sign of a sophisticated actor who has access to a stockpile of many such vulnerabilities and knows how to use them, which itself is a nontrivial problem because there is no manual or vendor testing for zero days. After a successful exfiltration, cyber spies face the same problems of any intelligence discipline: triaging unreliable sources, discovering useful data in terabytes of garbage, disseminating relevant analysis to fickle customers, remaining vigilant for counterintelligence exploitation. There is plenty of evidence that Chinese APTs conduct ambitious campaigns, but less evidence that Chinese firms have been able to make use of stolen data to catch up with, much less bypass, their Western competitors (Lindsay and Cheung, 2015).

Cyberwarfare, a term used here to describe the physical disruption of hardware connected to computer networks, adds additional operational cost and risk atop the challenges of espionage. Attackers first rely on prior network reconnaissance for target intelligence, and then on many of the same intelligence techniques to place a payload of malicious code onto the target network, which may be isolated across a so-called air gap. Yet, they must also engineer a specialized payload customized to the peculiarities of industrial control systems (ICS) or military command and control systems (C4ISR). The hacking skills needed

to spelunk across the internet hourglass and through the Windows software stack are different from the skills needed to understand how to manipulate factory machinery or weapons systems (Langner, 2013; Weiss, 2010).

The follow-through problem is particularly important in cyberwarfare, and its difficulty varies with the political-military purpose of the attack. An isolated surprise attack will only hurt and anger the target, leaving it time to investigate the attack, attribute the attacker, repair the damage and devise a response. Anything less than an incapacitating bolt from the blue against a wide range of military and industrial functions – a prohibitive engineering challenge for cyber warriors let alone a fleet of strategic bombers – will tend to stiffen the target's resolve for retaliation, as Japan learned after Pearl Harbor (Gartzke, 2013). By contrast, a surprise attack that is integrated with other military instruments to create a temporary window of vulnerability in enemy posture can be tactically useful (Libicki, 2007). Israel allegedly used cyberwarfare to shut down Syrian early warning radars for its raid on a Syrian nuclear facility in 2007 (Fulghum, 2007). Russian DDoS attacks against the government of Georgia in 2008 may have been synchronized with the Russian invasion as a form of barrage jamming to confuse Georgian communications (Deibert *et al.*, 2012). Yet, if the success of the military operation depends on the success of the cyberattack – as the Israeli strike arguably did and the Russian invasion did not – then it is imperative that commanders have confidence that the cyberattack will succeed in synchrony with other tactical events. A tactically useful weapon is one that creates a predictable effect at a predictable time and place without creating undesirable side-effects elsewhere. Commanders can have confidence in general purpose munitions tested in advance on a range, but there is much more uncertainty associated with a uniquely tailored and complex deception that may have potential for undesirable collateral effects. Unpredictable violence (or fizzle) does not make for a militarily useful weapon (Buchanan, 2017; Herrick and Herr, 2016). This is not only a difficult engineering and testing problem for cyber operators, but also difficult planning and control problem for commanders and operators (Slayton, 2017). The control systems of a fifth-generation fighter might be sabotaged in advance to ground the fleet, but if this tactical window is not exploited, then the target has the opportunity to investigate, attribute, recover from and respond to the attack. Both isolated and integrated surprise attacks are likely to be usable one time only, as the deception on which they depend is revealed through their use.

Another alternative is to use cyberwarfare not for tactical surprise but to inflict chronic friction in the material capabilities of the target. Restraint becomes important here for maintaining persistence. Too much damage or violence turns the sabotage into an isolated surprise attack, with the drawbacks just mentioned. Conversely, insufficient levels of damage submerge the deceptive gambit into the background levels of friction that the target already has to deal with in the course of normal operations. Chronic deceptive sabotage aims to preserve the cooperation that is the condition for its possibility, but doing so risks indistinguishability from normal benign cooperation. Cyberwarfare for covert sabotage must produce a Goldilocks balance of chronic attrition that is sustainable through deception and yet still politically useful. Stuxnet was caught on the horns of this dilemma (Lindsay, 2013). As a result, it contributed only marginally to US counter-proliferation efforts. The operation was arguably much more helpful for restraining Israel from conducting an airstrike against Natanz, which would have torpedoed the diplomatic process. The USA could credibly share the details of its deception with its Israeli co-conspirator without compromising the operation. Stuxnet enabled the USA to reassure Israel that is was doing something, even if that something ultimately had little effect on Iranian enrichment.

Sociotechnical counterinsurgency

Users, firms and governments place ever more trust in cyberspace, so there is phenomenal potential for deception. Yet, the sociotechnical processes that underwrite this trust become limiting liabilities for the attacker. Hackers have more in common with intelligence or terrorist operatives in an alien society who must depend on their wits and tradecraft to survive, as contrasted with uniformed soldiers who can call for fire support to reduce enemy resistance. The latter can use material power to impose their own rules and norms, operating within a friendly military hierarchy to overpower the adversary from the outside. The former must work within the rules and norms of the alien host society to survive the attention of more powerful security services. Subversives operate within the adversary's established institutions to undermine them from the inside. Furthermore, not all actors have the same skills or resources for deception, and security services will not be equally motivated to stop all actors. An ambitious operative who penetrates a powerful state faces a much harder problem than a petty criminal in that same state. The spy will not survive long against dedicated counterintelligence without training and support from a capable patron, while society will tolerate serious crime only as long as, unfortunately, its consequences are limited to the seedier side of town.

Network defenders have a difficult task because they have to maintain a sociotechnical infrastructure constructed and operated by a diverse community of actors. Inefficiencies in this environment provide opportunities for attackers, who then further weaken institutions by creating more inefficiency through their attacks. The defender has to coordinate with third parties in the system to repair the imperfections, if there is to be any hope of exposing and neutralizing hidden threat actors. This control contest bears a passing resemblance to the logic of counterinsurgency. The materially stronger incumbent relies on a strategy of institution building to obtain the information needed to find and defeat the rebel challenger, while the challenger improves its organizational capacity to survive underground and exploit the institutions built by the incumbent (Galula, 1964; Kitson, 1971; Taber, 1965; USA Army, 2006).

Given the mounting cost and risk associated with ambitious cyber operations, a very strong and very secretive organization is needed to subvert robust sociotechnical institutions. One of the greatest ironies of our age is that the most powerful spy agency in the most powerful country – the American NSA – is also the most adept at subverting the infrastructural commons that underwrites the American liberal economic order. The NSA is responsible for both signals intelligence and information assurance in the Department of Defense, i.e. offense and defense, and it leverages each of these missions to improve the other. The USA plays the role of both insurgent and counterinsurgent in cyberspace. The controversy surrounding civil liberties and the complicity of US firms in NSA espionage in the wake of the Edward Snowden leaks turns on whether these two roles are compatible. The insurgent role – covert espionage and disruption – is a mission that the NSA, along with USA Cyber Command in the same building, can better control; the cyber counterinsurgency depends on the help of many more actors, most of them in the private sector and increasingly suspicious of the NSA.

Cybersecurity as institution building

Despite all the attention to cyber insecurity, social trust in the internet continues its long-term increase as a constellation of institutional mechanisms stabilizes social and economic transactions at ever greater scale, speed and precision. The strongest indication of increasing trust is the online implementation of more and more economic functions – manufacturing, retailing, service, transportation, utilities, finance, etc. – together with new architectural and institutional innovations that emerge to span them or create wholly new functions (Chandler and Cortada, 2000; Cortada, 2012, 2008). Government administrators, corporate managers, advertising firms, factories and utilities, and the entertainment

industry are all increasing the scope and predictability of their operations. The universal improvement of control, however, creates control contests. The overlap and interference of different types of control systems with one another, and the intrusion of public control mechanisms into private realms where they were once absent, cannot help but generate controversy. Such are the politics of regulatory architecture and resource distribution in a maturing institutional system.

Emerging cyber threats are predicated on a broad general agreement about the desirability of a global knowledge infrastructure. Cyberspace is not governed by any single political authority, yet it is surely not anarchy. Extant cyber threats, such as they are, do not pose existential dangers in an anarchic system of self-help actors. Once the contractual nature of software and its supporting institutional ecosystem is appreciated, then the very term "cyber warfare" starts to look like an oxymoron. "Cyber" literally means "control", and control depends on the measurement, coordination and enforcement functions that institutions provide. By contrast, warfare erupts in anarchy and is out of control; otherwise, negotiation would prevail. No wonder cybersecurity typically deals with things other than war such as theft, fraud, espionage, propaganda, censorship and protest. These are all symptomatic of inefficiencies within an institutional system. Institutions are not free of politics, quite the opposite, but their struggles tend to focus on the efficiency of their design and the distribution of benefits, not existential survival. Control contests in and about cyberspace are either complicated disagreements about redistributive policies and sociotechnical architectures or opportunistic exploitations of institutional imperfections, not the violent existential conflicts of political anarchy. The proliferation of cyber threats, ironically, is predicated on increasing trust, stability and cooperation in the most complex political economic system that human beings have ever created.

Cybersecurity is not a new problem, but it continues to be a difficult one. Each generation of information technology affords new possibilities for efficient transactions, and therefore intelligence exploitation, which, in turn, demands better communication security (Headrick, 1991; Nickles, 2003). Military services, spy agencies, law enforcement and increasingly, private firms and citizens adapt these offensive and defensive potentials to advance and protect their political and economic interests. Competition among them results in an historical evolution that is anything but smooth, efficient and predictable in detail, yet this same evolution tends to ratchet up systemic complexity in the long run. The paradoxical result is that information technology both enhances control for its users and expands the contours of conflict between them. Sociotechnical complexity does create the potential for catastrophic failure (Perrow, 1999; Sagan, 1995; Snook, 2000; Vaughan, 1996); however, the severity of intentional conflict becomes more attenuated. Contemporary worries about ubiquitous mobile computing (smartphones), distributed software services and data warehousing (the cloud) and networks embedded in everyday appliances, vehicles and clothing (the Internet of things) will one day seem commonplace. Meanwhile, seemingly fantastic innovations, such as devices implanted in our bodies to alter our cognition or automated intelligences to replace us altogether, will generate more challenging variations on familiar themes. Security, not necessarily "cyber" security, is the underlying political economic problem, regardless of the material means in play.

The bargaining theory of war views uncertainty, whether a result of bluffing, secret capabilities, misperception or random error, as a source of conflict that prevents actors from reaching bargains they would prefer to war (Blainey, 1988; Fearon, 1995; Gartzke, 1999; Powell, 1999). The same insights inform the economic understanding of many market and government failures as a result of imperfect information (Coase, 1960; Stigler, 1961; Stiglitz, 2002). It is doubly unsurprising, therefore, that uncertainty should be a permissive cause of conflict involving information technology. Promising remedies for reducing cyber conflict, which may not necessarily be in the political interest of states like the USA, China and Russia that benefit from *sub rosa* exploitation campaigns, are thus informational in

nature. Standardized, public, empirical data on threat activity (rather than the present reliance on marketing material from cybersecurity firms and episodic media reporting) would go a long way toward enabling policy analysts to discern the nature and extent of market failure before rushing into regulatory solutions that could be counterproductive for innovation and security. At the same time, a counterintelligence approach to cybersecurity, which emphasizes active network monitoring, threat hunting and counterhacking, in effect using deception against the deceivers, has much promise for protecting public and private entities alike. Concerns about civil liberties and vigilantism are inevitable in any subversive contest and need to be actively managed, not assumed away.

Design inefficiencies in the sociotechnical fabric of cyberspace enable cheating within the institution, and actors struggle to redesign its normative and material constraints to curtail cheating. Deception becomes more sophisticated as sociotechnical hierarchies become better at guaranteeing the trust users place in them. Advanced digital threats are, ironically, symptomatic of the diminishing prospects of major warfare as a result of the growing power of states and their investment in a liberal economic order. The very developments that make information reliable on a massive and discriminating scale, improving commercial trade and military power projection, also diminish the utility of destructive revisionism. This should not be misunderstood as a claim that more information leads to reduced conflict, as greater transparency can also become a vector for malignant ideologies and misinformation (Lord, 2007). Rather, information improvements are correlated with other mechanisms that reduce the incentives for major conflict, i.e. the liberal or commercial peace and military deterrence. Downward pressure on the scale of aggression, for whatever reason, tends to increase the diversity and ambiguity of ambiguity of the revisionist challenges that remain. Not only is cyberspace correlated with developments that reduce incentives for war, cyberspace itself as a cooperatively constituted institution also creates incentives to moderate aggression via cyber means in war or any other time. Cyber conflict is restrained by design because actors have to cooperate to compete in cyberspace.

Notes

1. Valeriano and Maness (2015) describe "cyber restraint" as an empirical regularity and speculate about mechanisms that explain it ranging from deterrence, blowback, globalization and even a "cyber taboo". This paper offers a more parsimonious deductive explanation rooted in the institutional constitution of cyberspace.
2. Waltz uses the term "hierarchy" as the ideal type opposite to anarchy. I use the term "institution" instead to also include non-anarchic systems of rules that are not strict hierarchical relationships. In practice, sovereign states often adhere to norms, specialize functionally and assent to some degree of domination by others, so institutionalization is really a continuous variable (Lake, 2009), but it is traditionally most pronounced in domestic authority relations.
3. I thank Owen Cote, Jr for this turn of phrase.

References

Abelson, H., Anderson, R., Bellovin, S.M., Benaloh, J., Blaze, M., Diffie, W., Gilmore, J., Green, M., Landau, S., Neumann, P.G., Rivest, R.L., Schiller, J.I., Schneier, B., Specter, M. and Weitzner, D.J. (2015), "Keys under doormats: mandating insecurity by requiring government access to all data and communications", *Journal of Cybersecurity*, Vol. 1 No. 1, pp. 69-79.

Adair, S., Deibert, R., Rohozinski, R. and Villeneuve, N. (2010), "Shadows in the cloud: investigating Cyber Espionage 2.0.", Citizen Lab, Munk School of Global Affairs, University of Toronto, and SecDev Group, Toronto.

Agar, J. (2003), *The Government Machine: A Revolutionary History of the Computer*, MIT Press, Cambridge, MA.

Akerlof, G.A. (1970), "The market for 'lemons': quality uncertainty and the market mechanism", *The Quarterly Journal of Economics*, Vol. 84 No. 3, pp. 488-500.

Anderson, R. and Moore, T. (2006), "The economics of information security", *Science*, Vol. 314 No. 5799, pp. 610-613.

Asal, V., Mauslein, J., Murdie, A., Young, J., Cousins, K. and Bronk, C. (2016), "Repression, education, and politically motivated cyberattacks", *Journal of Global Security Studies*, Vol. 1 No. 3, pp. 235-247.

August, T. and Tunca, T.I. (2006), "Network software security and user incentives", *Management Science*, Vol. 52 No. 11, pp. 1703-1720.

Baldwin, C.Y. and Clark, K.B. (2000), *Design Rules: The Power of Modularity*, MIT Press, Cambridge.

Bauer, J.M. and van Eeten, M.J.G. (2009), "Cybersecurity: stakeholder incentives, externalities, and policy options", *Telecommunications Policy*, Vol. 33 Nos 10/11, pp. 706-719.

Bejtlich, R. (2013), *The Practice of Network Security Monitoring: Understanding Incident Detection and Monitoring*, No Starch Press, San Francisco.

Beniger, J.R. (1986), *The Control Revolution: Technological and Economic Origins of the Information Society*, Harvard University Press, Cambridge, MA.

Benkler, Y. (2006), *The Wealth of Networks: How Social Production Transforms Markets and Freedom*, Yale University Press, New Haven.

Benson, D.C. (2014), "Why the internet is not increasing terrorism", *Security Studies*, Vol. 23 No. 2, pp. 293-328.

Biddle, T.D. (2002), *Rhetoric and Reality in Air Warfare: The Evolution of British and American Ideas About Strategic Bombing, 1914-1945*, Princeton University Press, Princeton, NJ.

Blainey, G. (1988), *Causes of War*, 3rd ed., Simon and Schuster, New York, NY.

Bodmer, S., Kilger, M., Carpenter, G. and Jones, J. (2012), *Reverse Deception: Organized Cyber Threat Counter-Exploitation*, McGraw-Hill, New York, NY.

Borg, S. (2005), "Economically complex cyberattacks", *IEEE Security and Privacy Magazine*, Vol. 3 No. 6, pp. 64-67.

Bowden, M. (2011), *Worm: The First Digital World War*, Atlantic Monthly Press, New York, NY.

Bowker, G.C. and Star, S.L. (1999), *Sorting Things Out: Classification and Its Consequences*, The MIT Press, Cambridge, MA.

Brito, J. and Watkins, T. (2011), "Loving the cyber bomb: the dangers of threat inflation in cybersecurity policy", *Harvard National Security Journal*, Vol. 3 No. 1, pp. 39-84.

Brooks, Jr. and Frederick, P. (1995), *The Mythical Man-Month, Anniversary Edition: Essays on Software Engineering*, Anniversary Edition, Addison-Wesley Longman, Boston.

Brynjolfsson, E. and Saunders, A. (2010), *Wired for Innovation: How Information Technology is Reshaping the Economy*, MIT Press, Cambridge, MA.

Buchanan, B. (2017), *The Cybersecurity Dilemma: Hacking, Trust and Fear Between Nations*, Oxford University Press, New York, NY.

Carr, E.H. (1939), *Twenty Years' Crisis, 1919-1939: An Introduction to the Study of International Relations*, Macmillan & Co., London.

Chandler, A.D. and Cortada, J.W. (Eds) (2000), *A Nation Transformed by Information: How Information Has Shaped the United States from Colonial Times to the Present*, Oxford University Press, New York, NY.

Cherepanov, A. (2017), "WIN32/INDUSTROYER: a new threat for industrial control systems", ESET (accessed 12 June 2017).

Choucri, N. (2012), *Cyberpolitics in International Relations*, MIT Press, Cambridge, MA.

Cimbala, S.J. (2012), *Nuclear Weapons in the Information Age*, Continuum International Publishing, New York, NY.

Claffy, K. and Clark, D. (2014), "Platform models for sustainable internet regulation", *Journal of Information Policy*, Vol. 4, pp. 463-488.

Clarke, R.A. and Knake, R.K. (2010), *Cyber War: The next Threat to National Security and What to Do about It*, Ecco, New York, NY.

Coase, R.H. (1960), "The problem of social cost", *Journal of Law and Economics*, Vol. 3, pp. 1-44.

Cortada, J.W. (2008), *The Digital Hand*, Vol. 3, Oxford University Press, Oxford; New York, NY.

Cortada, J.W. (2012), *The Digital Flood: Diffusion of Information Technology Across the United States, Europe, and Asia*, Oxford University Press, Oxford; New York, NY.

Crosby, A.W. (1997), *The Measure of Reality: Quantification in Western Europe, 1250-1600*, Cambridge University Press, Cambridge.

Deibert, R.J., Rohozinski, R. and Crete-Nishihata, M. (2012), "Cyclones in cyberspace: information shaping and denial in the 2008 Russia-Georgia war", *Security Dialogue*, Vol. 43 No. 1, pp. 3-24.

Demchak, C.C. and Dombrowski, P.J. (2011), "Rise of a Cybered Westphalian Age", *Strategic Studies Quarterly*, Vol. 5 No. 1.

DeNardis, L. (2009), *Protocol Politics: The Globalization of Internet Governance*, MIT Press, Cambridge, MA.

DeNardis, L. (2014), *The Global War for Internet Governance*, Yale University Press, New Haven.

Deudney, D.H. (2007), *Bounding Power: Republican Security Theory from the Polis to the Global Village*, Princeton University Press, Princeton, NJ.

Deutsch, K.W. (1963), *Nerves of Government: Models of Political Communication*, Free Press, New York, NY.

Downey, G. (2001), "Virtual webs, physical technologies, and hidden workers: the spaces of labor in information internetworks", *Technology and Culture*, Vol. 42 No. 2, pp. 209-235.

Drezner, D.W. (2004), "The global governance of the internet: bringing the state back in", *Political Science Quarterly*, Vol. 119 No. 3, pp. 477-498.

Dunn Cavelty, M. (2008), "Cyber-terror – looming threat or phantom menace? The framing of the US cyber-threat debate", *Journal of Information Technology & Politics*, Vol. 4 No. 1, pp. 19-36.

Dupuy, JP. (2000), *The Mechanization of the Mind: On the Origins of Cognitive Science*, Princeton University Press, Princeton.

Durumeric, Z., Kasten, J., Adrian, D., Halderman, A., Bailey, M., Li, F. and Weaver, N. (2014), "The matter of heartbleed", *Proceedings of the 2014 Conference on Internet Measurement Conference, IMC '14*, ACM, New York, NY, pp. 475-488, doi: 10.1145/2663716.2663755.

Edelman, B. (2011), "Adverse selection in online 'trust' certifications and search results", *Electronic Commerce Research and Applications*, Vol. 10 No. 1, pp. 17-25.

Edwards, P.N. (2010), *A Vast Machine: Computer Models, Climate Data, and the Politics of Global Warming*, MIT Press, Cambridge, MA.

Edwards, B., Furnas, A., Forrest, S. and Axelrod, R. (2017), "Strategic aspects of cyberattack, attribution, and blame", *Proceedings of the National Academy of Sciences*, Vol. 114 No. 11, pp. 2825-2830.

Elliott, D. (2011), "Deterring strategic cyberattack", *IEEE Security & Privacy*, Vol. 9 No. 5.

Eriksson, J. and Giacomello, G. (2006), "The information revolution, security, and International Relations: (IR) relevant theory?", *International Political Science Review/Revue Internationale de Science Politique*, Vol. 27 No. 3, pp. 221-244.

Faughnder, R. (2015), "Sony co-chair Amy Pascal steps down after hacking scandal", *Los Angeles Times*, 5 February.

Fearon, J.D. (1995), "Rationalist explanations for war", *International Organization*, Vol. 49 No. 3, pp. 379-414.

FireEye Threat Intelligence (2015), *HAMMERTOSS: Stealthy Tactics Define a Russian Cyber Threat Group*, FireEye, Milpitas, CA.

Fulghum, D.A. (2007), "Why Syria's air defenses failed to detect Israelis", Aviation Week, Ares Blog, 3 October.

Galula, D. (1964), *Counterinsurgency Warfare: Theory and Practice*, Praeger Security International, Westport, CT.

Gartzke, E. (1999), "War is in the error term", *International Organization*, Vol. 53 No. 3, pp. 567-587.

Gartzke, E. (2007), "The capitalist peace", *American Journal of Political Science*, Vol. 51 No. 1, pp. 166-191.

Gartzke, E. (2013), "The myth of Cyberwar: bringing war in cyberspace back down to earth", *International Security*, Vol. 38 No. 2, pp. 41-73.

Gartzke, E. and Lindsay, J.R. (2015), "Weaving tangled webs: offense, defense, and deception in Cyberspace", *Security Studies*, Vol. 24 No. 2, pp. 316-348.

Gartzke, E. and Lindsay, J.R. (2017), "Thermonuclear Cyberwar", *Journal of Cybersecurity*, Vol. 3 No. 1, pp. 37-48.

Gat, A. (2006), *War in Human Civilization*, Oxford University Press, New York, NY.

Glaser, C.L. (2010), *Rational Theory of International Politics: The Logic of Competition and Cooperation*, Princeton University Press, Princeton, NJ.

Global Research & Analysis Team (2015), "Equation: the death star of malware galaxy", *Securelist, Kaspersky Labs*, 16 February.

Goldsmith, J.L. and Wu, T. (2006), *Who Controls the Internet? Illusions of a Borderless World*, Oxford University Press, New York, NY.

Gompert, D.C. and Libicki, M. (2014), "Cyber warfare and Sino-American crisis instability", *Survival*, Vol. 56 No. 4, pp. 7-22.

Grindal, K. (2013), "Operation Buckshot Yankee", in Healey, J. (Ed.), *Fierce Domain: Conflict in Cyberspace, 1986 to 2012*, Cyber Conflict Studies Association, Washington, DC, pp. 205-211.

Haggard, S. and Lindsay, J.R. (2015), "North Korea and the Sony hack: exporting instability through cyberspace", Asia Pacific Issues No. 117, East-West Center, Honolulu, HI.

Hallam-Baker, P. (2013), "Nation-state attacks on PKI", *Lecture presented at the RSA Conference*, San Francisco, CA, 27 February.

Hao, S., Borgolte, K., Nikiforakis, N., Stringhini, G., Egele, M., Eubanks, M., Krebs, B. and Vigna, G. (2015), *Drops for Stuff: An Analysis of Reshipping Mule Scams*, ACM, Denver, pp. 1081-1092.

Haun, P.M. (2015), *Coercion, Survival, and War: Why Weak States Resist the United States*, Stanford University Press, Stanford, CA.

Hayden, M.V. (2016), "The making of America's cyberweapons", *Christian Science Monitor*, 24 February.

Headrick, D.R. (1991), *The Invisible Weapon: Telecommunications and International Politics, 1851-1945*, Oxford University Press, New York, NY.

Healey, J. (Ed.) (2013), *A Fierce Domain: Conflict in Cyberspace, 1986 to 2012*, Cyber Conflict Studies Association, Washington, DC.

Herley, C. (2013), "When does targeting make sense for an attacker?", *IEEE Security & Privacy*, Vol. 11 No. 2, pp. 89-92.

Herley, C. and Florêncio, D. (2010), "Nobody sells gold for the price of silver: dishonesty, uncertainty and the underground economy", in Moore, T.W., Ioannidis, C. and Pym, D.J. (Eds), *Economics of Information Security and Privacy*, Springer, New York, NY, pp. 33-53.

Herrick, D. and Herr, T. (2016), "Combating complexity: offensive cyber capabilities and integrated warfighting", Atlanta.

Hess, C. and Ostrom, E. (Eds) (2007), *Understanding Knowledge as a Commons: From Theory to Practice*, MIT Press, Cambridge, MA.

Hurwitz, R. (2012), "Depleted trust in the cyber commons", *Strategic Studies Quarterly*, Vol. 6, pp. 20-45.

Ikenberry, G.J. (2001), *After Victory: Institutions, Strategic Restraint, and the Rebuilding of Order after Major Wars*, Princeton University Press, Princeton.

Ikenberry, G.J. (2009), "Liberal internationalism 3.0: America and the dilemmas of liberal world order", *Perspectives on Politics*, Vol. 7 No. 1, pp. 71-87.

Jervis, R. (1978), "Cooperation under the security dilemma", *World Politics*, Vol. 30 No. 2, pp. 167-214.

Kello, L. (2013), "The meaning of the cyber revolution: perils to theory and statecraft", *International Security*, Vol. 38 No. 2, pp. 7-40.

Keohane, R.O. (Ed.) (1986), *Neorealism and Its Critics*, Columbia University Press, New York, NY.

Keohane, R.O. and Martin, L.L. (1995), "The promise of institutionalist theory", *International Security*, Vol. 20 No. 1, pp. 39-51.

Keohane, R.O. and Nye, J.S. (2001), *Power and Interdependence*, Longman, New York, NY.

Kitson, F. (1971), *Low Intensity Operations: Subversion, Insurgency and Peacekeeping*, Stackpole, Harrisburg, PA.

Kline, R.R. (2015), *The Cybernetics Moment: Or Why We Call Our Age the Information Age*, Johns Hopkins University Press, Baltimore.

Knockel, J., McKune, S. and Senft, A. (2016), "Baidu's and don'ts: privacy and security issues in Baidu browser", Citizen Lab Report, University of Toronto Munk School of Global Affairs, Toronto.

Lake, D.A. (2009), *Hierarchy in International Relations*, Cornell University Press, New York, NY.

Landau, S.E. (2010), *Surveillance or Security? The Risks Posed by New Wiretapping Technologies*, MIT Press, Cambridge, MA.

Langner, R. (2013), *To Kill a Centrifuge: A Technical Analysis of What Stuxnet's Creators Tried to Achieve*, The Langner Group, Virginia.

Latour, B. (1987), *Science in Action: How to Follow Scientists and Engineers through Society*, Harvard University Press, Cambridge, MA.

Lawson, S. (2013), "Beyond cyber-doom: assessing the limits of hypothetical scenarios in the framing of cyber-threats", *Journal of Information Technology & Politics*, Vol. 10 No. 1, pp. 86-103.

Lessig, L. (2006), *Code*, 2nd ed., Basic Books, New York, NY.

Leyla, B. and Tudor, D. (2012), "Before we knew it: an empirical study of zero-day attacks in the real world", *Proceedings of the ACM Conference on Computer and Communications Security*, Raleigh, NC, pp. 833-844.

Libicki, M.C. (2007), *Conquest in Cyberspace: National Security and Information Warfare*, Cambridge University Press, New York, NY.

Libicki, M.C. (2009), *Cyberdeterrence and Cyberwar*, RAND, Santa Monica, CA.

Libicki, M.C. (2012), *Crisis and Escalation in Cyberspace*, RAND Corporation, Santa Monica, CA.

Liff, A.P. (2012), "Cyberwar: a new 'absolute weapon'? The proliferation of cyberwarfare capabilities and interstate war", *The Journal of Strategic Studies*, Vol. 35 No. 3, pp. 401-428.

Lindsay, JR. (2013), "Stuxnet and the limits of cyber warfare", *Security Studies*, Vol. 22 No. 3, pp. 365-404.

Lindsay, JR. (2015), "Tipping the scales: the attribution problem and the feasibility of deterrence against cyber attack", *Journal of Cybersecurity*, Vol. 1 No. 1, pp. 53-67.

Lindsay, J.R. and Cheung, T.M. (2015), "From exploitation to innovation: acquisition, absorption, and application", in Lindsay, J.R., Cheung, T.M. and Reveron, D.S. (Eds), *China and Cybersecurity: Espionage, Strategy, and Politics in the Digital Domain*, Oxford University Press, New York, NY.

Lindsay, J.R. and Gartzke, E. (2017), "Coercion through cyberspace: the stability-instability paradox revisited", in Greenhill, K.M. and Krause, P.J.P. (Eds), *Coercion: The Power to Hurt in International Politics*, Oxford University Press, New York, NY.

Lord, K.M. (2007), *The Perils and Promise of Global Transparency: Why the Information Revolution May Not Lead to Security, Democracy, or Peace*, State University of New York Press, Albany, NY.

Lupovici, A. (2014), "The 'attribution problem' and the social construction of 'violence': taking cyber deterrence literature a step forward", International Studies Perspectives.

Mackenzie, D.A. (1990), *Inventing Accuracy: A Historical Sociology of Nuclear Missile Guidance*, MIT Press, Cambridge, MA.

Markoff, J. (2008), "Huge system for web surveillance discovered in China", *The New York Times*, 1 October.

Mearsheimer, J.J. (1994), "The false promise of international institutions", *International Security*, Vol. 19 No. 3, pp. 5-49.

Medina, E. (2011), *Cybernetic Revolutionaries: Technology and Politics in Allende's Chile*, MIT Press, Cambridge, MA.

Messerschmitt, D.G. and Szyperski, C. (2003), *Software Ecosystem: Understanding an Indispensable Technology and Industry*, MIT Press, Cambridge, MA.

Moe, T.M. (1990), "Political institutions: the neglected side of the story", *Journal of Law, Economics, & Organization*, Vol. 6, pp. 213-253.

Molnar, D., Egelman, S. and Christin, N. (2010), "This is your data on drugs: lessons computer security can learn from the drug war", *Proceedings of the 2010 Workshop on New Security Paradigms, NSPW '10, ACM, New York, NY*, pp. 143-149.

Morris, I. (2014), *War! What Is It Good For? Conflict and the Progress of Civilization from Primates to Robots*, Farrar, Straus and Giroux, New York, NY.

Mueller, J.E. (2004), *The Remnants of War*, Cornell University Press, Ithaca.

Mueller, M.L. (2010), *Networks and States: The Global Politics of Internet Governance*, MIT Press, Cambridge, MA.

Nelson, N. (2016), *The Impact of Dragonfly Malware on Industrial Control Systems*, InfoSec Reading Room, SANS Institute, Prague.

Nickles, D.P. (2003), *Under the Wire: How the Telegraph Changed Diplomacy*, Harvard University Press, Cambridge, MA.

North, D.C. (1990), *Institutions, Institutional Change, and Economic Performance*, Cambridge University Press, New York, NY.

Obama, B. (2012), "Taking the Cyberattack threat seriously", *Wall Street Journal*, 19 July.

Olson, M. (1965), *The Logic of Collective Action*, Harvard University Press, Cambridge, MA.

Ostrom, E. (1990), *Governing the Commons: The Evolution of Institutions for Collective Action*, Cambridge University Press, New York, NY.

Pape, R.A. (1996), *Bombing to Win: Air Power and Coercion in War*, Cornell University Press, Ithaca, NY.

Perrow, C. (1999), *Normal Accidents: Living with High Risk Technologies*, 2nd ed., Princeton University Press, Princeton, NJ.

Peterson, D. (2013), "Offensive cyber weapons: construction, development, and employment", *Journal of Strategic Studies*, Vol. 36 No. 1, pp. 120-124.

Pinker, S. (2011), *The Better Angels of Our Nature: Why Violence Has Declined*, Penguin New York, NY.

Powell, R. (1999), *In the Shadow of Power: States and Strategies in International Politics*, Princeton University Press, Princeton, NJ.

Railton, J.S. and Kleemola, K. (2015), *London Calling: Two-Factor Authentication Phishing From Iran*, University of Toronto Munk School of Global Affairs, Citizen Lab, Toronto.

Rattray, G.J. (2001), *Strategic Warfare in Cyberspace*, MIT Press, Cambridge, MA.

Rattray, G., Evans, C. and Healey, J. (2010), "American security in the cyber commons", in Denmark, A.M. and Mulvenon, J. (Eds), *Contested Commons: The Future of American Power in a Multipolar World*, Center for a New American Security, Washington, DC, pp. 137-176.

Rid, T. (2012), "Cyber war will not take place", *The Journal of Strategic Studies*, Vol. 35 No. 5, pp. 5-32.

Rid, T. (2016), *Rise of the Machines: A Cybernetic History*, W. W. Norton & Company, New York, NY.

Rid, T. and Buchanan, B. (2015), "Attributing cyber attacks", *Journal of Strategic Studies*, Vol. 38 Nos 1/2, pp. 4-37.

Rosenzweig, P. (2013), *Cyber Warfare: How Conflicts in Cyberspace Are Challenging America and Changing the World*, Praeger, Santa Barbara, CA.

Rovner, J., Lindsay, J.R., Marten, K. and O'Rourke, L.A. (2017), "Russia and the 2016 US Presidential Election", ISSF Policy Roundtable 1-7, *H-Diplo*, available at: https://networks.h-net.org/node/28443/discussions/173096/issf-policy-roundtable-1-7-russia-and-2016-us-presidential

Rushe, D. (2015), "The interview revenge hack cost Sony just $15m", *The Guardian*, 4 February 4, sec. Film.

Sagan, S.D. (1995), *The Limits of Safety: Organizations, Accidents, and Nuclear Weapons*, Princeton University Press, Princeton, NJ.

Sanger, E.L., David, E. and Shane, S. (2016), "The perfect weapon: how Russian cyberpower invaded the US", *The New York Times*, New York, NY, 13 December.

Schelling, T.C. (2008), *Arms and Influence: With a New Preface and Afterword*, Yale University Press, New Haven, CT.

Schmidt, A. (2013), "The Estonian cyberattacks", in Healey, J. (Ed.), *A Fierce Domain: Conflict in Cyberspace, 1986 to 2012*, Cyber Conflict Studies Association, Washington, DC, pp. 174-193.

Schmidt, E. and Cohen, J. (2013), *The New Digital Age: Reshaping the Future of People, Nations and Business*, Alfred A. Knopf, New York, NY.

Scott, J.C. (1998), *Seeing Like a State: How Certain Schemes to Improve the Human Condition Have Failed*, Yale University Press, New Haven, CT.

Scott-Railton, J., Marquis-Boire, M., Guarnieri, C. and Marschalek, M. (2015), *Packrat: Seven Years of a South American Threat Actor*, University of Toronto Munk School of Global Affairs, Citizen Lab, Toronto.

Shapiro, C. and Varian, H.R. (1999), *Information Rules: A Strategic Guide to the Network Economy*, Harvard Business School Press, Cambridge, MA.

Slantchev, B.L. (2011), *Military Threats: The Costs of Coercion and the Price of Peace*, Cambridge University Press, New York, NY.

Slayton, R. (2017), "What is the cyber offense-defense balance? Conceptions, causes, and assessment", *International Security*, Vol. 41 No. 3, pp. 72-109.

Snook, S.A. (2000), *Friendly Fire: The Accidental Shootdown of U.S. Black Hawks Over Northern Iraq*, Princeton University Press, Princeton, NJ.

Sowell, J.H. II (2015), "Finding order in a contentious internet", Ph.D. dissertation, Engineering Systems Division, MA Institute of Technology, MA.

Starrs, S. (2013), "American economic power hasn't declined – it globalized! Summoning the data and taking globalization seriously", *International Studies Quarterly*, Vol. 57 No. 4, pp. 817-830.

Stigler, G.J. (1961), "The economics of information", *Journal of Political Economy*, Vol. 69 No. 3, pp. 213-225.

Stiglitz, J.E. (2002), "Information and the change in the paradigm in economics", *The American Economic Review*, Vol. 92 No. 3, pp. 460-501.

Taber, R. (1965), *War of the Flea*, L. Stuart, New York, NY.

USA Army (2006), *FM 3-24: Counterinsurgency*, Government Printing Office, Washington, DC.

Valeriano, B. and Maness, R. (2014), "The dynamics of cyber conflict between rival antagonists, 2001-2011", *Journal of Peace Research*, Vol. 51 No. 3, pp. 347-360.

Valeriano, B. and Maness, R.C. (2015), *Cyber War versus Cyber Realities: Cyber Conflict in the International System*, Oxford University Press, New York, NY.

Vaughan, D. (1996), *The Challenger Launch Decision: Risky Technology, Culture, and Deviance at NASA*, University of Chicago Press, Chicago.

von Neumann, J. and Morgenstern, O. (1944), *Theory of Games and Economic Behavior*, Princeton University Press, Princeton, NJ.

Wagner, R.H. (2000), "Bargaining and war", *American Journal of Political Science*, Vol. 44 No. 3, pp. 469-484.

Waltz, K.N. (1979), *Theory of International Politics*, Addison-Wesley Publication, Reading, MA.

Weiss, G.W. (1996), "The farewell dossier: duping the soviets", *Studies in Intelligence*, Vol. 39 No. 5.

Weiss, J. (2010), *Protecting Industrial Control Systems from Electronic Threats*, Momentum Press, New York, NY.

Williamson, O.E. (1981), "The economics of organization: the transaction cost approach", *American Journal of Sociology*, Vol. 87 No. 3, pp. 548-577.

Winner, L. (1980), "Do artifacts have politics?", *Daedalus*, Vol. 109 No. 1, pp. 121-136.

Zetter, K. (2015), "How the secretive market for zero-day exploits works", *Slate*, 24 July.

Zetter, K (2016), "Inside the cunning, unprecedented hack of Ukraine's power grid", *Wired*, 3 March.

Zittrain, J.L. (2006), "The generative internet", *Harvard Law Review*, Vol. 119 No. 7, pp. 1974-2040.

Corresponding author

Jon Randall Lindsay can be contacted at: jon.lindsay@utoronto.ca