Journal of Global Security Studies, 2(3), 2017, 184–203
doi: 10.1093/jogss/ogx008
Research Article

OXFORD

Does the Internet Need a Hegemon?

Joshua Rovner[1] and Tyler Moore[2]

[1]Southern Methodist University and [2]University of Tulsa

Abstract

Hegemonic stability theory holds that a dominant power can produce international cooperation by providing public goods and resolving collective action dilemmas. Successful hegemons also resist the temptation to exploit their advantages in order to reduce other states' fear of domination. This article asks whether or not the internet needs the United States to play a similar role. If so, Washington should pursue policies designed to strengthen internet security while eschewing espionage and cyberattacks that rely on some degree of internet insecurity. If not, it can go on the offensive without fear of undermining the system as a whole. We examine the technical and political fallout from revealed offensive cyberoperations to assess the relative fragility of the internet. Our findings suggest that it is relatively resilient.

Keywords: Cybersecurity, hegemonic stability theory, offensive cyber operations, Stuxnet, Snowden

Cybersecurity is a US national interest and a global public good. The United States has powerful economic reasons to support a secure and reliable internet, given the amount of commerce and intrafirm business now conducted online. It also has a strong military stake in cybersecurity, given the scope and complexity of communications among military forces and along the chain of command. Cybersecurity is a global public good because it enables access to reliable communications for all users. Everyone benefits from efforts to mitigate vulnerabilities in software code, for instance, whether or not they paid for them. And the worldwide boom in online communications means that securing the internet protects the global economy.

But cybersecurity comes at a cost. The same protections that enable individuals to communicate safely also enable criminals and militants to hide online. In addition, while Washington has a clear interest in cybersecurity, it also seeks to conduct espionage and attack its rivals in cyberspace. Offensive cyberoperations (OCO) are a particularly appealing alternative to war as they avoid the costs and risks of military violence. Perfect cybersecurity would make such operations impossible. Other states know this, of course, which causes them to question US motives. Indeed, the fact that cybersecurity is a global public good does not mean that international cybersecurity cooperation is inevitable, nor that other states welcome US assistance. Fears of state intervention have raised concerns that the internet, once seen as an apolitical bastion of free thought and exchange, will become fragmented as states use it for their own purposes.

The clash of national and global interests in cyberspace is particularly acute because there is no global government to resolve disputes. Sustaining cooperation under anarchy is an enduring puzzle for international relations theorists and animates some of the most enduring debates in political science. Realist scholars view the international system as prone to conflict because there is no higher authority that can enforce agreements among states (Waltz 1979). Liberal theorists, however, posit that international institutions can foster cooperation in part by reducing transaction costs (Keohane 1984). Extensions of this debate, including arguments about the value of institutions, are discussed below. But perhaps the most controversial argument focuses on the role of a hegemon, or a clearly dominant state, in the international system. Hegemonic stability theory (HST) posits that peace and

This research was supported by the National Science Foundation, Award #SES-1444863.

Rovner, Joshua and Tyler Moore. (2017) Does the Internet Need a Hegemon?. *Journal of Global Security Studies*, doi:10.1093/jogss/ogx008

prosperity are more likely when there is a clear hierarchy of states and one undisputed leader. A state with dominant capabilities can sustain cooperation by providing public goods and reducing collective action problems. Incentives to cheat on agreements or free ride are reduced when the hegemon picks up the tab. Hegemons also help coordinate action and deter challengers from threatening the global order.

Some critics of HST argue that hegemony is destabilizing because any state with a preponderance of power will create fear and suspicion among others. Anarchy will compel smaller and weaker states to protect themselves against a predatory hegemon, either by building up their own defenses or by forming balancing alliances. However, defenders note that the hegemon can take steps to reduce such fears by binding itself to international bodies or designing political institutions that constrain leaders, including its own, from rash decisions. Others acknowledge that, while a hegemon may be necessary for establishing order in a deeply unstable environment, it will become less important over time. The emergence of durable international institutions will encourage cooperation after hegemony by improving the quality of information available and by reducing transaction costs. In either case, the dominant power sustains the international order by eschewing parochial actions. Resisting the temptation to exploit its power encourages cooperation by reducing smaller states' fear of domination.

Contemporary critics might doubt whether or not the United States maintains the ability to play the role of benevolent hegemon, particularly since recent events suggest it cannot protect its own critical systems. During the 2016 presidential campaign, the Russian government allegedly organized the theft of emails from the Democratic National Committee and Hillary Clinton's campaign chairperson John Podesta. It subsequently used WikiLeaks and other websites to publish the contents online as part of an effort to embarrass Clinton and sow doubt about US institutions. Donald Trump won the election by a very narrow margin, and some observers believe that his victory would have been impossible without Russian interference. Most significantly, US intelligence and law enforcement agencies were unable to prevent the cyberheist, and the Obama administration offered a tepid and vacillating response. This is not the portrait of a state able to play the hegemon on this issue. If anything, the election drama suggests that the United States is playing catch-up. The notion that the United States can provide cybersecurity as a global public good seems increasingly absurd.

But the events of last summer need be put in context. The Russian operation was a modern version of an old political tool Soviet officials call "active measures." These mostly included propaganda and misinformation designed to bring down government officials, candidates for office, and other prominent political figures. Historically, the record of Soviet active measures against the United States was quite poor (Andrew and Mitrokhin 1999). This time proved different, but had little to do with US cybercapabilities. Instead, it was largely a product of one of the strangest campaigns in US history, including a series of unlikely events that came together to enable Russian efforts and promote Trump's eventual victory.[1] Moreover, even if the United States is vulnerable to propaganda, this does not mean it is less able to influence global cybersecurity. By way of analogy, we do not doubt the fighting strength of the US military based on civilian vulnerability to terrorist attacks.

For reasons of history, geography, and technology, the United States continues to enjoy an extraordinary position in cyberspace. US computer scientists built the internet and experienced predominant influence over the design of institutions that currently govern it. Meanwhile, the National Security Agency (NSA) emerged as the largest signals intelligence organization in the world, investing in extraordinary capabilities for espionage, information assurance, and OCO. Silicon Valley remains the hub for global private sector technology development. And both government and industry benefit from American higher education, which has expanded graduate programs in computer science and related fields. These capabilities remain unaffected by the events of last year. While US influence might decline over time, especially if other states build capabilities that make cooperation with the United Sates unnecessary, so far this has not occurred.

How might the United States use these unique capabilities? Informed by the assumption that cybersecurity is a public good prone to collective action, most see a tradeoff between US investments in cyberattacks and espionage for its national security benefit and continued provision of a secure internet for the world. Those advocating for internet security suggest that Washington (1) increase its involvement in internet governance in order to help

[1] Perhaps the most important was Federal Bureau of Investigation (FBI) Director James Comey's letter to the House Judiciary Committee eleven days before the election. Comey revealed that the Bureau had possession of new emails that might be pertinent to the months-long investigation of Clinton's use of a private email server. Earlier Comey had put to rest speculation that Clinton would face an indictment, but the letter reignited the controversy, breathing new life into the Trump campaign (McElwee, McDermott, and Jordan 2017).

codify a set of durable rules of the road or (2) decide to give up opportunities for espionage and sabotage by strengthening encryption, alerting technology firms to vulnerabilities in software and taking additional steps to make internet communications inviolable—or both.

Here we use an empirical investigation of response to significant security failures to evaluate whether or not this trade-off is really in effect. We propose five measures of internet resiliency and evaluate the aftermath of the Stuxnet attack on Iran's nuclear complex and the Snowden revelations about the NSA. Did these events lead to significant changes in user, firm, and state behavior? Such changes would suggest that cybersecurity is vulnerable to collective action problems, or perceived as such, and that great powers risk undermining the security of the internet when they use it as a vehicle for intelligence gathering and covert operations. On the other hand, the *absence* of significant behavioral change in the wake of Stuxnet and Snowden suggests that fears that cyberattacks will lead to erosion of the public good may be exaggerated. In this case, the United States could more safely pursue its dual interests without fear of eroding cybersecurity.

We proceed in three steps. The first section describes HST and applies it to cyberspace. While new technologies have led some to question the relevance of classic international relations theories, we explain why HST offers a useful framework for the cybersecurity policy debate. The second section explores the cases in detail. We find that the internet proved resilient, despite fears that OCO would undermine the cooperation needed to sustain it. This is significant both for what it suggests about the consequences of OCO, but also because the current debate exists mostly in the abstract. Policy arguments about internet security primarily weigh the possible effects of US policy, instead of studying the outcomes achieved so far. The conclusion discusses those outcomes and describes the implications for international relations (IR) theory and US cybersecurity policy.

Hegemonic Stability Theory

HST holds that international politics are stable when there is one dominant state in the international system. The theory came to prominence following the Great Depression, when political economists bemoaned the lack of a leader who could stabilize the global economy and prevent what amounted to a systemic bank run[2]. More recently, scholars have speculated that the theory might also apply to international security, pointing to periods of hegemony like the Pax Britannica of the nineteenth century when a dominant power provided security and discouraged arms racing and other actions that might have led to crises and war.[3]

Scholars have criticized HST on both logical and empirical grounds. Balance of power theorists argue that a preponderance of power is actually *destabilizing* because it provokes fear among weaker states. Other critics have noted that, for the theory to succeed, the hegemon must agree to reduce its relative power by subsidizing others. This amounts to self-defeating behavior that could lead to dangerous power shifts. Other scholars offer more conditional criticisms of HST. Keohane (1984) notes that while hegemons are able to provide stability in emerging systems for which conditions are fragile, they are not needed to maintain stability in deeply institutionalized political orders because the conditions for keeping such systems afloat are far less demanding. Ikenberry (1998–99, 2000) similarly argues that hegemons can bind themselves to international institutions in order to alleviate fears about intentions.

Critics of all stripes note that there is not a lot of empirical support for the original version of the theory, at least not at the systemic level.[4] Recent studies suggest, though, that it does explain regional outcomes.[5] For example, Great Britain and the United States have alternated as the naval hegemon of the Persian Gulf since the end of World War II through the provision of public goods in the form of political stability and oil security (Rovner and Talmadge 2014).

[2] The classic treatments are Kindleberger (1973) and Gilpin (1981).

[3] For a concise application to security studies, see Sheetz (1997–98).

[4] Critiques from the interprofessional education literature include Snidal (1985), McKeown (1983), and Gowa (1989). For IR critiques, see Ikenberry (1998–99) and Drezner (2013). For an argument about how beliefs about hegemony underlie the major debates over US grand strategy, see Avey, Markowitz, and Reardon (2017).

[5] Other international relations theorists have explained how "nested" systems can exist within the larger international system. Bipolarity best describes the geopolitics of East Asia, for example, with China as the dominant land power and the United States as the leader at sea. The balance persists despite vast US advantages over all other states. Thus regional bipolarity can exist within an unipolar system (Ross 1999).

Public Goods and Collective Action Dilemmas

HST assumes that collective action problems will interrupt the global supply of public goods. We say something is a public good if it is non-rival and non-excludable. It is non-rival because one person's consumption does not interfere with another's and non-excludable because no one can be denied consumption. Clear air is a common example of a public good. Individuals do not compete for access to clean air, and all enjoy the benefit.[6]

Cybersecurity comes close to a public good. A perfectly secure and reliable global internet would enable universal and unrestricted access.[7] Yet without cybersecurity, the internet may not function in this manner. One user's access to the internet does not preclude anyone else from logging on, of course, but the depletion of Internet Protocol (IP) version 4 addresses does create a competitive market for internet access. And while some argue that internet access *should* be nonexcludable, the fact is that there *are* practical ways to deny access to users. For example, many recommendations for protecting intellectual property online involve efforts to take down illegal content or to prevent users from visiting certain websites. There are also cases of states shutting down web services, thus denying access to their citizens. Some have warned about the possible "Balkanization" of the internet by states who do not want to expose themselves to foreign intelligence collection or cyberattack, and authoritarian states like China have aggressively censored content for many years as a way of restricting information and controlling political debate.

Cybersecurity includes a raft of goods: threat information sharing, secure networks, firewalls, intrusion detection systems, and a variety of hardware and software tools designed to fend off cyberattacks and mitigate the consequences. Some of these, like threat information sharing, are clearly public goods. The benefit of public information sharing by definition is nonexcludable and nonrivalrous. Reliable domain name server routing and autonomous systems connectivity also qualify as public goods.

However, other aspects of cybersecurity are closer to nonrival but excludable club goods. Password-protected secure networks, for instance, increase cybersecurity only to members. While increasing the security of a single firm's computer systems does not preclude other firms from making the same investments, the protections often stop at the firm's network perimeter. A displacement effect is further possible when any individual or organization invests in security. The protection of property reduces the available number of targets by one, which makes those remaining more conspicuous and tempting for attackers. This is especially problematic if the pool of available targets is so small that individual decisions affect the security level of all others. Alongside private actors, states may also enhance cybersecurity by censoring content or sharply reducing public access as a means of reducing opportunities for intrusion by malicious actors.

Another argument against viewing cybersecurity as a public good is that, while public goods should be prone to underprovision because of incentives to free ride, private firms have invested heavily in cybersecurity (Powell 2005; Rosenzweig 2011; Raymond 2013). Such high levels of private investment may correspond to circumstances in which the investment elevates cybersecurity of the individual firm in an excludable fashion, as in the case of club goods. Furthermore, high rates of investment do not necessarily indicate the absence of a market failure. Indeed, where externalities are present, the level of private investment may still be less than what is socially optimal when information asymmetries regarding the effectiveness of cybersecurity investments lead to ineffective spending (Anderson and Moore 2006). Hence, spending large sums provides no guarantee that firms are spending effectively (Moore, Dynes, and Chang 2016).

These arguments notwithstanding, there are powerful reasons to think of cybersecurity as a public good. While access to the internet may be excludable, cybersecurity in the broadest sense is not; everyone's security improves when states arrest cybercriminal gangs, patch vulnerabilities in widely used software, and so on. It is also nonrivalrous in that one user's improved security does not come at the expense of another's security. Moreover, the global economy increasingly relies on it. According to one study, the global digital economy was set to surpass $20 trillion in 2013, the equivalent of nearly 14 percent of total world trade (Oxford Economics 2011). Because of long and complex global supply chains, few individuals and firms would be spared from a serious and prolonged interruption of internet services, even those who do little direct business online. Thus while reliable internet access is sometimes excludable, everyone would suffer if it became less secure.

[6] Common examples of public goods are national defense and clean air. Gilpin (1987, 74) offers other examples that are more pertinent to this study: an open trade regime based on the principle of nondiscrimination and unconditional reciprocity, a stable international currency, and international security.

[7] For related arguments, see McPherson and Zimmerman (2010), Mulligan and Schneider (2011), and Chucri (2012, 170–71, 236–37).

In sum, cybersecurity benefits all users when they can communicate safely online, allowing buyers to shop safely and firms to receive payment. Most directly, it prevents fraud and abuse and enables international trade and finance. It allows users to communicate over vast distances in real time and provides a staggering amount of information at very little cost. Conversely, cyber*insecurity* puts trade and finance at risk while inhibiting the flow of information for all users. For these reasons, it makes sense to think of cybersecurity as a public good.

The other building block of HST is the role of hegemonic leadership in overcoming collective action problems, which loom large in questions about cybersecurity and internet governance. Major decisions about internet rules are the product of international coordination between numerous organizations and individuals. States play a role but not a dominant one; firms and institutions, including the Internet Engineering Task Force and the Internet Corporation for Assigned Names and Numbers, make most internet governance decisions. Relevant parties are investing heavily with such organizations over the debate surrounding online communications. Civil libertarians fiercely guard against any encroachment on what they see as a bastion of free expression, while firms see opportunities for commercial gain, with considerations surrounding impacts on intellectual property. Finally, while some states view the internet as a vehicle for public diplomacy and cultural exchange, they also fear exposure to espionage while providing asymmetric opportunities for weaker adversaries who otherwise would not pose much of a threat. As a result, states have become less willing to leave responsibilities to the private sector. They all believe the stakes are high, but have very different interests, making collective action increasingly difficult.[8]

The ongoing debate about the appropriate level of state intervention is actually a debate about whether or not the internet can function on its own. Optimists believe it can, arguing that the internet has proven remarkably self-regulating and resilient to shocks via informal rules of governance that have encouraged a free flow of information and innovation. Optimists further posit that firms and internet users have enormous incentives to keep the system running, regardless of how states behave. The sheer scale of online communications and commerce means that they are willing to pay the costs and provide the technical experience needed to keep the internet secure and reliable. Cyberattacks may temporarily disrupt service, but the system as a whole will continue to function because motivated actors will expedite efforts to strengthen cyberdefenses and restore access. Perhaps the internet is similar to oil security, another public good that has proved resilient without hegemonic protection (Gholz and Press 2010).[9] If the optimists are correct, there is no need for a hegemon to ensure the health of the internet. Washington could feel more confident about attacking its own rivals in cyberspace—much as navies attack one another on the ocean—without fear that it will inadvertently damage the broader internet.

Others argue that the internet is inherently vulnerable. Built without attention to security and vulnerable to predation, any decline in interstate cooperation will lead global communications to fragment. Unlike the international waters upon which oil tankers transit, the internet is a human construct requiring constant attention and maintenance. By definition, it is not self-sustaining. Moreover, the apolitical origins of internet governance and the unusual characteristics of internet organizations suggest that it cannot rely on a foundation of institutional institutions to guarantee cooperation.

If the pessimists are correct, a cavalier attitude toward cyberspace could lead to long-term disruption with serious economic and political consequences (Corera 2015). To keep global cybersecurity intact, the United States should forego opportunities for OCO and cyberespionage, because the system is too fragile to survive if the dominant state is insensitive to the fallout from its own self-serving actions.

Is the Internet's Security Fragile?

Two recent revelations of clandestine US efforts to penetrate or attack information systems previously assumed to be secure provide an opportunity to measure the internet's fragility. The first is the Stuxnet attack against Iran's nuclear program. The second involves former NSA contractor Edward Snowden's revelations about the agency in 2013. We describe the response in both cases. The basic test is simple: if the optimists are right, then these cases should not have dramatically dampened enthusiasm for internet communications and commerce. But dramatic changes, including signs of retrenchment from users, firms, and states, would indicate that cybersecurity depends on hegemonic restraint.

[8] An added complication is that state intervention could be more or less helpful in different aspects of internet governance. Preserving the Transmission Control Protocol (TCP)/IP, for instance, requires little help from states. For this reason, even a well-intentioned state could prove to have ineffectual leaders if they carelessly intervene. We thank an anonymous reviewer for this observation.

[9] For critiques, see Levi (2013, 132–38) and Yetiv (2015).

We develop and employ five measures of fragility to assess the unintended results of Stuxnet and the Snowden revelations. The first three are political, and the last two are technical. The internet operates as a kind of global common, which only exists because of human engineering and maintenance. Thus, a useful analytical framework must also pay attention to the technical details of internet operations, both before and after political shocks. Our approach relies in equal measure on IR theory, political economy, and computer science.

To be clear, we do not attempt to address all aspects of cybersecurity. Our conception relies on a classic construct, abbreviated CIA, which stands for confidentiality, integrity, and availability. Cybersecurity obtains when all three goals are achieved. In the ideal, users safely communicate without risking unauthorized disclosure of information, without having that information modified or erased, and without being denied access to information or information systems.[10] Because a sufficient technical analysis is beyond the scope of this article, we focus squarely on resilience as the most germane to understanding the fallout from OCO. Describing and measuring resilience in these cases is crucial for understanding cybersecurity in periods during which observers fear that cyberspace has become *insecure*.

The following section outlines the measures we employ. After introducing the categories, we report on the data observed in the context of Stuxnet and the Snowden disclosures. The evidence is not comprehensive, of course, as both events were recent. Moreover, we do not claim that Stuxnet and Snowden are perfectly representative of all conceivable cyberattacks. However, the logic of the framework is generalizable. Indeed, by describing broad political and technical measures of fragility, we believe it provides a useful framework for analyzing political and technological responses to similar incidents. We summarize the framework in Tables 1 and 2.

User Responses

The first measure of fragility is user responses to revelations of cyberattacks and espionage that may affect innocent third parties. Targeted OCO can inadvertently infect tens of thousands of computers, even when operations are designed to affect particular facilities and designers tailor malicious code for specific systems. Similarly, signals intelligence agencies like the NSA may deliberately undermine encryption or stockpile software vulnerabilities in order to ensure they can continue to exploit cyberspace for espionage. This may be particularly troubling to innocent users, who assume some level of privacy (Schneier 2015).

The most straightforward means of measuring user response is by tracking usage rates in the wake of major controversies. Flat or declining usage would suggest decreasing trust in the security of online communications, which in turn would imply system fragility. On the other hand, continued increases or stability in the number of users, as well as the amount of time users spend online, would imply that state activities have little effect. Users may be unaware of OCO or unconcerned. In either case, the fact that they continue logging on is an indication of resilience.

Simply logging on, however, normally carries little risk of surveillance by governments or exploitation by criminals. The risk increases when users participate in online commerce, engage in frequent and wide-ranging use of social media, share personal information, perform searches on controversial topics, and or engage in political debate. Users can participate more or less energetically, and their decisions affect their level of exposure. Thus, the relevant question is not simply whether or not controversies affect usage rates, but how they influence users' online habits. Their awareness of aggressive state action in cyberspace may lead them to believe that their data is easily compromised and may be used against them. Concerned users may choose a full retreat from the internet or take less extreme albeit noticeable steps to reduce internet activity. For example, they may reduce user-to-user communication via email, Skype, and social media. Such changes suggest less confidence in cybersecurity due to fears of government intrusion.

Users may also reduce online spending where providing personal and financial information in cyberspace is required. Decreasing levels of commerce would therefore indicate that the trust needed to sustain the system is eroding. Increased consumer spending on cyberdefenses, along with a more widespread adoption of encryption, similarly indicates reduced levels of trust. This measure is not dispositive, however, as the implications cut in both directions. Greater investment in cyberdefenses may be a sign that users are less confident in cybersecurity and feel the need to ramp up security efforts. However, it is also a possible indication of internet resiliency as a sign that non-state actors respond to security threats in ways that specifically avoid state assistance. They are sufficiently confident in the system that they are willing to go it alone.

Firm Responses

The second fragility measure focuses on the behavior of firms, including those that play a direct role in cybersecurity and those that conduct a substantial portion of

[10] Singer and Friedman (2014) provide a primer on the technical issues associated with cybersecurity.

their business online. Evidence of resiliency would include signs that firms are nonplussed about revelations of cyberespionage and OCO. If they view such actions as par for the course and do not adjust levels of commerce and online communication, they are likely to have confidence in the underlying resilience of the internet. Evidence for firm responses is both qualitative (e.g., public statements made by corporate leaders) and quantitative (e.g., online sales as a percentage of total business). Therefore, unlike individual users, it is unclear that increasing investment in cyberdefenses is a good indirect measure of internet fragility. A sudden increase in spending in the wake of controversies might indicate a worrisome sign of distrust, but could also signal that firms are simply committed to the internet and doing what they deem necessary to protect it preemptively, regardless of any one particular controversy. By way of analogy, businesses often install new locks to keep out thieves without waiting for an increase in local robberies.

In this regard, the behavior of information technology (IT) firms is particularly important given their role in producing and maintaining the technology that makes the internet possible. Such firms have long cooperated with the government on various issues relating to cybersecurity, but often have mixed incentives. On the one hand, they seek to maintain good relations because government agencies are both regulators and consumers of their products. However, they also have obligations to comply with lawful orders, meaning they cannot shun agencies even if relations are hostile. That said, there are limits to what is legally required, and firms prefer to preserve an image of independence. A reputation for being too close to the government might increase fears of government intrusion and alternatively decrease consumer confidence in their products designed to keep the internet secure, reliable, and safe from prying eyes. As a result, revelations of supposed state misconduct might lead firms to move even further away from their government counterparts for fear of losing domestic and foreign market share. This in turn might discourage the kind of public-private cooperation needed to locate, arrest, and prosecute cybercriminals. The ultimate result would be a lower level of internet security in general.

State Responses

Our third measure of fragility focuses on state responses to revelations of US actions. States are particularly important because they have the ability to block user access to large amounts of content. Such decisions could "Balkanize" the internet, effectively destroying the goal of an international forum for the free exchange of ideas, goods, and services. A decline in interstate cooperation would further inhibit responses to cybercrime, especially if law enforcement requires joint efforts for seizing and extraditing cybercriminals. More broadly, a decline in cooperation could affect issues ranging from attribution of cyberattacks to coordinated responses.

We measure state responses by evaluating interaction changes with known practitioners of espionage and OCO. States may view such actions as a normal part of political life such that revelations are unlikely to affect their level of cooperation. Espionage is nothing new, after all, and political officials may brush off cyberspying as nothing more than that which is politically routine. On the other hand, the scope and potential consequences of such activities might strike them as fundamentally different given the nature of the technologies involved and their own increasing dependence on the internet. If this is the case, states may reduce ongoing cooperative efforts and abandon new initiatives. This would represent an erosion of cybersecurity.

States can reduce cooperation in several ways. First, they can limit the quality and quantity of participation in law enforcement collaborations on cybercrime. Significant criminal enterprises, such as botnets, often cross geopolitical borders and require multinational cooperation to combat. We can trace variation in the breadth and depth of this kind of collaborative law enforcement to assess the second-order international effects of targeted cyberoperations. If the effects are severe, we should see fewer and less intensive joint efforts.

Second, states can reduce cooperation on incident response. A variety of private sector and national computer security incident response teams (CSIRTs) work to mitigate the damage of cyberattacks. They also serve a prophylactic purpose by educating public and private sector actors about security risks and issuing advisories about hardware and software vulnerabilities. International cooperation among CSIRTs helps improve both the speed and comprehensiveness of responses to malicious attacks. Subsequently, a reduction in cooperation could lead to more widespread and damaging attacks and lengthen the average recovery time.

Third, states can back away from moves toward international regulatory harmonization on internet standards. Specifically, they can reduce participation in multistakeholder meetings that attempt to set rules on a range of issues, including how to assign IP addresses and how to restrict bulk email messages. As these issues devolve to state authorities, it may prove increasingly difficult to coordinate internationally on internet security. Routine collaboration may serve to grease the wheels for cooperation on more sensitive issues. Habitual interaction on related issues may facilitate efforts to shore up cybersecurity or to respond to cyberattacks.

The most serious responses are deliberate efforts to reduce state exposure to the internet in order to protect against foreign intelligence gathering or sabotage. The danger of such closures will increase if states believe that exerting sovereignty online is the prudent response to a world in which great powers are using cyberspace against them. As one observer puts it, "The fundamental challenge of aspiring to a global, open Internet is that Beijing, Moscow, and others see it as a threat to their national security and as inordinately benefiting Washington strategically, economically, and politically" (Segal 2016, 233). This problem might not stop with US adversaries. Indeed, allies and neutral states might fear that they too cannot escape the potential for cyberattacks. Just as cybersecurity is a nonexcludable public good, cyberinsecurity is a nonexcludable public harm. Thus, they may raise their own defenses, thereby creating a world of national intranets, rather than a globally interconnected system, even at the risk of substantial political and economic harm.

Incident Responses

In addition to behavioral responses, we employ technical indicators to measure resilience. We first consider the prevalence of and recovery from incidents themselves. The Stuxnet attack triggered retaliatory attacks from Iran against US banks and the oil company Saudi Aramco. What was the effect of the denial-of-service attacks against the banks, and did the harm persist or attenuate over time? What was the response time for Saudi Aramco to resume operations and recover from the lost data? If the effects of such attacks were devastating and increasingly severe, this would suggest fragility. If the victims adapted to the attack and took steps to mitigate future harm, it would be a sign of resilience.

In addition to retaliatory attacks, other types of technical responses can be observed to gauge fragility or resilience. By way of example, the network routing protocol border gateway protocol (BGP) remains vulnerable to impersonation attacks that trigger temporary outages. While such attacks cannot be prevented, they can set off a rapid international response from network operators to correct the problem. Subsequently, the prevalence of BGP outages is an indicator of the ongoing tension between the defenders of computer networks and those who seek to impose damage. If these attacks take place with greater frequency, it suggests that the internet is becoming more fragile. Likewise, stable or decreasing response times suggest resiliency.

Finally, episodes of data breaches provide indirect evidence about cybersecurity writ large. When firms lose control of digital records containing personal information, even if only temporarily, this indicates poor security practices. Because most US states now require customer notification when personal information is revealed, we can reliably measure the frequency and severity of breaches, along with responses. More losses imply insecurity if the numbers outpace in the total number of users, as this reflects an inability to proactively adjust protection measures as usage expands. The absolute number of data breaches matters less than the loss of user information relative to the growth of the internet.

Infrastructure Responses

Lastly, we examine how the information and computing technologies infrastructure has changed. Stuxnet exploited several known zero-day vulnerabilities, and the Snowden revelations showed that such vulnerabilities were sought and used by NSA. Hence, a natural way to understand resilience is to examine the process of identifying and fixing such flaws. For example, we can measure the time between the discovery of vulnerabilities and the publication and distribution of patches that plug the holes. If most vulnerabilities are patched quickly and the fixes are widely disseminated, this suggests resilience even in the face of persistent state efforts to use them against rivals.

While software vulnerabilities can be corrected by installing a patch, secure system, configuration usually requires more judgment and active participation from those managing the infrastructure. For example, many critical infrastructure operators connect industrial control systems to the internet, either for reasons of convenience or by accident. The Stuxnet attacks may have served as a wake-up call to critical infrastructure operators that they should take computer system security more seriously. One way to measure this is to compare the number of industrial control systems that are connected to the internet now versus when the Stuxnet attack first went public. If that number has fallen, it would be a sign of resilience; if it has risen, it would indicate fragility.

Similarly, website operators can minimize exposure by supporting encryption via a secure hypertext transfer protocol (HTTPS). An increase in encrypted web traffic suggests increased security and resilience by offering protections against surveillance and data breaches. A related issue is the type of encryption supported by websites implementing HTTPS. Before 2011, most HTTPS implementations did not guarantee perfect forward secrecy (PFS). In effect, without PFS, an adversary who compromised an encryption key could decrypt all traffic observed that was encrypted using the key. However, some forms of key exchange do achieve PFS. In this case, when an encryption key is compromised, only communications from

Table 1. Political measures

	Evidence of fragility	Evidence of resilience
Users	Flat or declining usage	Rising usage
	Flat or declining online purchasing	Rising online purchasing
	Reduced variety of online activities and platforms	Increased variety of online activities and platforms
	Reluctance to engage in political debate or share personal information	Enthusiasm for political debate and willingness to share personal information
Firms	Public or private statements from corporate leaders expressing doubt	Public or private statements from corporate leaders expressing confidence
	Lack of public statements demonstrating cybersecurity investment in response to OCO	Public statements demonstrating cybersecurity investment in response to OCO
	Flat or declining online sales as a percentage of the total	Rising online sales as a percentage of the total
	Flat or declining reliance on cyberspace for intrafirm operations (e.g., supply chain management)	Rising reliance on cyberspace for intrafirm operations
	Reduced willingness of IT firms to cooperate with government	Continued willingness to cooperate with government
States	Reduced international legal cooperation with alleged authors of OCO	Steady or increasing legal cooperation
	Reduced cooperation on incident response	Steady or increasing incident response cooperation
	Moves away from regulatory harmonization	Enthusiasm for regulatory harmonization
	Balkanization	Openness

the current web session can be decrypted. Subsequently, increased support for HTTPS communications with PFS would indicate resilience.

Notably, not all infrastructure changes improve resiliency. Consider the effect of concentrations in the internet's routing topology. For a variety of reasons, Internet service providers (ISPs) may choose to reduce the number of public-facing internet connections (i.e., border routers). Doing so makes the internet more fragile because it makes it easier for a single actor—be it a government actor or individual attacker—to disrupt or surveil internet connections. One could therefore measure the changing topology by inspecting the routes advertised using BGP.

Stuxnet and Snowden

For about two months beginning in late 2009, the Stuxnet worm attacked Iranian centrifuges at the Natanz enrichment plant. The centrifuges spin uranium gas at supersonic speeds in order to capture specific isotopes capable of undergoing fission. The facility requires precise timing to coordinate the actions of thousands of centrifuges, which collect increasing amounts of fissile uranium as the gas is fed and recycled. At the time of Stuxnet, this process was particularly important to Iran as it was the only facility enriching uranium to add to the Iranian stockpile.[11] Sabotage to Natanz could slow or halt Iran's effort to accumulate sufficient fissile material for nuclear weapons.

The Stuxnet attack was complex and clever. The operation was designed to cripple the accumulation of fissile uranium in a manner that looked like normal wear and tear. No one would suspect sabotage, leaving the facility vulnerable to continued attacks. Pulling off such an operation required detailed knowledge of the control systems at Natanz including the ability to report back, meaning the first part of the operation was infiltrating the air-gapped facility to install what became known as the "Stuxnet beacon." Once completed, the worm began to start and stop the centrifuges to increase fatigue over a period of months without alerting site engineers that anything was wrong. Ultimately, the worm disabled around

[11] Iranian engineers did not begin feeding nuclear material into the Fordow plant until late 2011 (International Atomic Energy Agency 2013).

Table 2. Technical measures

	Evidence of fragility	Evidence of resilience
Incident responses	Slow recovery from attacks	Rapid recovery from attacks
	Operations not fully restored	Operations fully restored
	More frequent BGP attacks; slow responses	Less frequent BGP attacks; rapid responses
	Rising data breaches as a percentage of total users	Flat or declining data breaches as a percentage of total users
Infrastructure responses	Software patches disseminated and applied inefficiently	Software patches disseminated and applied efficiently
	Increased number of industrial control systems connected to the internet	Reduced number of connected industrial control systems
	Decrease in encrypted web traffic	Increase in encrypted web traffic

one thousand centrifuges during the attack window, or about one fifth of the total at Natanz.

Despite these clandestine efforts, private security firms discovered the virus in June 2010. Observers soon began debating the operational consequences. Some saw Stuxnet as a harbinger of new warfare and proof that cyberattacks could cause meaningful physical damage. Furthermore, they worried similar worms could become weapons of the weak against industrial control systems in large industrialized economies (Zetter 2014). Skeptics, however, noted that very few states or nonstate actors had the financial resources and technological wherewithal to choreograph such a complicated attack. Moreover, the attack itself had a small effect on Iran's nuclear program. Quite counterintuitively, Iran actually increased its fissile material stockpile during the two months the worm was operating. Seen in this light, Stuxnet suggests that OCO is a tool of the strong to score small victories against the weak (Lindsay 2013; Valeriano and Maness 2015).

Stuxnet ultimately spread far outside of Natanz. Forensic investigations found that it infected over 100,000 hosts in 155 states (Zetter 2011; Falliere, Murchu, and Chien 2011). Keeping worms from spreading beyond their intended target is inherently difficult, meaning attackers risk such negative externalities. As one researcher put it, malware is akin to chemical or biological weapons, which are hard to control and potentially lethal to foe and friend alike (Espiner 2012). In the aftermath of Stuxnet, security analysts warned that future attacks could have wide-ranging effects, including a cyberarms race among states who might otherwise have worked together to strengthen the internet and norms inhibiting OCO. "Rather than treating cyberspace as a neutral realm of information exchange and innovation, Stuxnet opened the doors for ongoing cyberwar—a siege that puts critical civilian infrastructure at substantial risk" (Landale and Meinrath 2015).

Similar concerns arose the following summer. In early June 2013, the *Guardian* published a story on the NSA's collection of telephone metadata within the United States (Greenwald 2013). This was the first of many revelations over the next several months based on information stolen by NSA contractor Edward Snowden. In addition to the initial disclosure, Snowden revealed a wealth of classified information about a variety of other signals intelligence programs. Much of the controversy about the disclosures had to do with the NSA's domestic programs, especially its metadata program. The majority of the revealed programs, however, were against foreign targets. It was these programs as much as anything else that caused concern that the United States and US-based technology companies were collaborating in ways that threatened the security and reliability of the internet.

The Snowden revelations led some observers to conclude that the NSA was guilty of serious abuses that betrayed the Constitution and threatened civil liberties. Others argued that they highlight the degree to which the notion of online privacy is an illusion. The NSA's ability to intercept commercial hardware and surreptitiously implant custom devices, as well as its alleged effort to install malware in firmware, suggests that its surveillance may be both widespread and undetectable. The other accusations—that the NSA was stockpiling zero-days, looking for backdoors, and undermining encryption—all add up to a collective warning to users about the dangers of communicating online.[12]

The extraordinary events of 2012 and 2013 led critics to warn that intelligence agencies were making a mockery of the notion of an open, secure, and reliable internet. According to one observer, "Year Zero" demolished the

[12] For a good summary of these charges, see Segal (2016, 119–28). For an extended warning about the risks of surveillance, see Schneier (2015).

wistful notion of cyberspace as an apolitical domain. Rather, "nation-states around the world visibly reasserted their control over the flow of data and information in search of power, wealth, and influence, finally laying to rest the already battered myth of cyberspace as a digital utopia, free of conventional geopolitics. The assault on this vision was comprehensive, global, and persistent" (Segal 2016, 1).

But the reaction of users, firms, and governments suggests the consequences were less severe. First, there is no evidence that users backed away from online communications and commerce because of the Stuxnet and Snowden revelations. The total number of worldwide internet users rose from just over two billion in 2010 to over three billion in 2015. Around half a billion new users logged on between 2011 and 2012, suggesting that there was no widespread fear that Stuxnet or its successors would threaten the integrity of the internet. Expansion continued apace even after the Snowden revelations (Statista 2015).

Users risk little for logging on, but they face more dangers that are serious when they begin conducting business. There is no evidence, however, that Stuxnet or Snowden discouraged users from buying and selling online. Retail e-commerce in the United States, for instance, rose 3.8 percent from 2012 to 2013. In countries hit particularly hard by Stuxnet, like India, there is even evidence that a majority of users were unaware of the attack just months after the US role was revealed (Madaan 2012). This was certainly not for lack of media coverage, as users simply might have been uninterested, nor did firms change their behavior in the aftermath. Wholesale and manufacturing sales online rose dramatically during the same period (US Census Bureau 2015).

Furthermore, neither individual users nor firms retreated from the internet despite fears of malware contagion. Some increased their investment in various forms of cybersecurity, a trend that has continued to the present (Kim 2015). A smaller number also became interested in encrypted communications, causing concern among intelligence and law enforcement officials who feared that the expansion of encryption would make it more difficult to prevent attacks or prosecute criminals. This in turn set off a particularly intense debate over the intersection between privacy and security in online communication. But while end-to-end encryption techniques were impressive, it was not clear they were widely in use or whether or not the Snowden revelations produced a sudden surge of interest.

To investigate whether or not mobile apps promising secure communications have increased in popularity since 2013, we inspected historical rankings of the top 500 paid and top 500 free applications in the communications category of Google Play, the Android app store. We collected the top-1,000-ranked apps (500 free, 500 paid) on July 1 of each year, from 2012 to 2016, as reported by appannie.com. We counted all apps that included the words "privacy," "private," and "encrypt" in their name, excluding apps that were browsers or virtual private networks (VPNs). In total, we found twenty-two private SMS and phone apps.

Table 3. Android private messaging or phone applications

	2012	2013	2014	2015	2016
# apps (# free)	6 (3)	7 (5)	7 (6)	8 (5)	13 (9)
Top-ranked app	129	99	168	151	81
Median rank	326	326	122	189	294

Source: appannie.com.

Table 3 shows the breakdown by year. The total number of private communications apps grew from six in 2012 to thirteen in 2016. The top-ranked free application also increased from 129 in 2012 to 99 in 2013, before falling again from 2014 to 2015. During this time, the popularity of the top-ranked free application, Signal Private Messenger, which uses pairwise symmetric encryption with keys known only to the users in communication, steadily increased. According to the Google Play store, Signal was installed between one and five million times since its introduction in 2012. While that is impressive, it should also be put in context: the top apps on the Google Play store have been installed between one and five *billion* times. Notably, the use of private communications apps, while growing, has not expanded dramatically since the Stuxnet and Snowden revelations.

While some individuals became more concerned about cybersecurity, their numbers are small compared with the overall growth of internet users. A cross-national survey of college students, for example, found that respondents were generally aware of the Snowden revelations and that some had changed their online practices as a result. In particular, researchers found that students who knew about Snowden took steps ranging from changing privacy settings to reducing the use of personal devices. But the specific changes are unclear. In New Zealand, for example, 59 percent of the respondents who were aware of the controversy indicated that they had altered their communications practices, but only 6 percent elaborated on the particular steps. Likewise, roughly half of the Spanish students reported doing everything from paying more attention to changing privacy settings and erasing personal data. But the study failed to report the percentages of respondents who chose more or less extreme measures. Moreover, it relied on small numbers—fewer than one hundred students responded in more than half of the surveys—and it is unclear that college students are representative of the larger population. As the researchers acknowledge, their efforts reflect a "snapshot" of perceptions and behaviors after Snowden, rather than a detailed analysis of users' communications practices (Adams et al. 2015; Gunasekara et al. 2015; Oliva et al. 2015).

Other studies have found that user behavior changed after 2013, though the effects again appear quite modest. Almost two years after the Snowden revelations, the Pew Research Center conducted a survey to measure American responses to accusations of government surveillance. The survey found that while nine out of ten Americans had heard about the controversy, only three out of ten had changed their behavior online. Moreover, the steps they took were often restricted to simple measures like selecting passwords that were more complex. Only a minority of respondents took steps that were more stringent. For example, 15 percent reported using social media less often and 14 percent said they were communicating more in person (Rainie and Madden 2015). A separate survey found that similarly sized groups were avoiding online searches for terms that might be personally embarrassing or politically dangerous. Most importantly, data from Google Trends showed roughly a 10 percent decline in search terms that might lead to government scrutiny, and a somewhat smaller decline for search terms that might be embarrassing. This is evidence that intelligence revelations did produce a "chilling effect," but only for a small minority of individual users (Matthews and Tucker 2015).

Firms responded to the news of Stuxnet in different ways. Unsurprisingly, those offering cybersecurity services pointed to the worm as another sign of the growing dangers online. The more interesting question is whether the broader business community changed its attitude toward cooperation with the government. Such cooperation is crucial not least because firms possess threat information based on attacks on their networks. This information is important for states as they develop threat profiles of foreign attackers, which is important for defending the private and public sectors.

The involvement of state actors did cause concern among some firms that worried whether or not they could keep up a suitable defense against military-backed adversaries. At a meeting of industry leaders and researchers convened by the Department of Homeland Security (DHS) to discuss impediments to the adoption of cyberinsurance, a "plurality of the participants" deemed as uninsurable due to "catastrophic risks for which most believed the federal government should be responsible" including state-sponsored computer viruses (US Department of Homeland Security 2012). Attendees also noted that some insurers had already begun excluding from coverage acts of cyberwar, though it is unclear whether a Stuxnet-like attack would fall under cyberwar.

We do not observe clear evidence that firms changed their behavior with respect to public-private partnerships related to cybersecurity. Quite simply, information sharing between the private and public sectors was problematic long before Stuxnet or Snowden. A 2010 Government Accountability Office report noted that most private sector companies felt the US government was not providing timely and actionable cybersecurity threat information (US Government Accountability Office 2010). Furthermore, many private sector firms were reluctant to share information with the federal government due to liability concerns and fear of public disclosure. If anything, coordination may have improved in recent years, despite Stuxnet, because DHS has made concerted efforts to meet the expectations of private-sector firms. Sector-specific information sharing and analysis centers continue to operate, though no public data is available on whether membership has grown.

Useful data regarding this interaction comes from large tech companies, which regularly publish the number of requests for user data made by governments and courts.[13] We analyzed data published by Google, Apple, Microsoft, and Facebook. Figure 1 plots Google's compliance rate over time for a selection of states. Here the compliance rate is defined as the percentage of government requests that result in data turnover. Overlaid on the plot are indications of when Stuxnet and the Snowden disclosures were first made public. While there is considerable variation in compliance by the requests' country of origin, fulfillment is relatively steady over time. Requests from the United States have the highest level of compliance, though the rate has declined from more than 90 percent in the second half of 2010 to around 80 percent today. Requests from India, by contrast, have declined from 80 percent to around half. Most noteworthy, though, cooperation between Google and other countries post-Snowden has not diminished, even though Google arguably has incentives to resist cooperation in order to regain consumer trust.

[13] Secondary analysis and amalgamation of data gathered from https://www.google.com/transparencyreport/userdatarequests/, https://govtrequests.facebook.com/, https://www.microsoft.com/about/csr/transparencyhub/lerr/, https://www.apple.com/privacy/transparency-reports/.

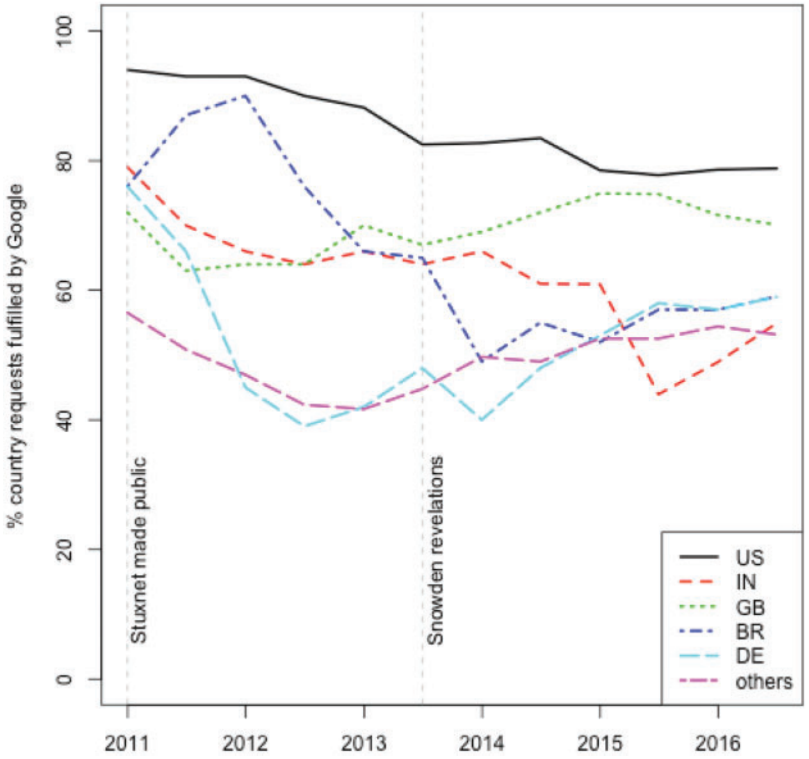

Figure 1. State-level breakdown of Google's compliance with requests for user data.

Figure 2 examines the global compliance rate with law enforcement requests for data from four major US tech companies. Apple, Facebook, and Microsoft began publishing data on law enforcement requests around the same time that the Snowden disclosures surfaced. This is likely not a coincidence and might have been an attempt to regain customer trust through increased transparency. Nonetheless, the companies continued to cooperate with law enforcement at similar rates over time. Again, this suggests that, for government interaction, firms have not substantially changed their behavior.

Many of the first responders to cyberincidents work for CSIRTs. Governments run some CSIRTs; sectoral groups, private firms, and software vendors run others. CSIRTs process reports of newly discovered vulnerabilities, including the Stuxnet attack, and share findings with affected vendors and the public. Successful CSIRTs have gained the trust of those who discover software flaws, leading some to fear that Stuxnet may reduce that trust. Indeed, in a study of CSIRT activity conducted in 2015, Skierka et al. (2015) found that "in interviews, most practitioners noted that even the suspicion of complicity with questionable law enforcement or intelligence practices could be enough to ruin trust in teams and undermine cooperation" (21).

Stuxnet likely contributed to the explosion of "bug bounty" programs, in which technology firms offer financial rewards to researchers who find vulnerabilities in their software. While this was a natural response, firms were reticent to explain their motives. For example, while not explicitly acknowledging Stuxnet, Google established a bug bounty program in November 2010 (Google n.d). Other firms followed thereafter, indicating that such programs might function as public signals demonstrating firms' cybersecurity investments. Such commitments improve resiliency and patch vulnerabilities, including threats like Stuxnet.

States responded to Stuxnet by increasing investment in offensive and defensive cybersecurity techniques, but few reduced cooperation with the United States. By way of example, the FBI published nearly 700 press releases about ongoing and completed cybersecurity investigations from 2004 to 2016. Of these, 121 included some international law enforcement cooperation, ranging from arrests and interdictions to collaborative investigations. More than half of all instances of cooperation occurred

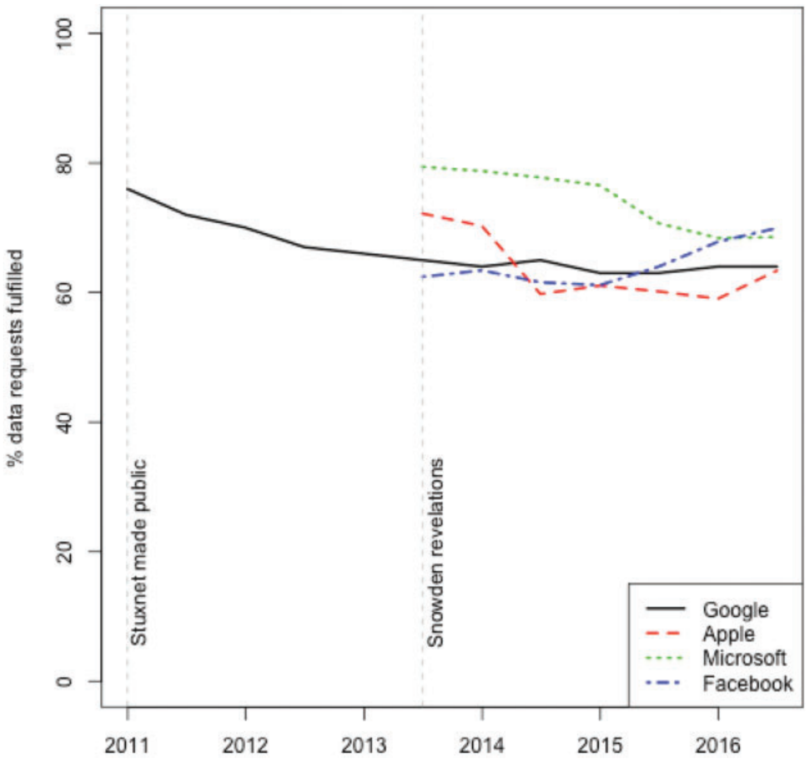

Figure 2. Global compliance rates with law enforcement requests for data from Google, Apple, Microsoft and Facebook.

after US involvement in Stuxnet was revealed in June 2012. The expansion of internet usage makes a rise in cooperative efforts likely, to be sure, because more cybercrime means more cyberinvestigations. Still, the evidence does not suggest that revelations of US OCOs affected the willingness of other states to work with American law enforcement.[14]

Consider the reactions of a US ally (Great Britain), an affected third-party (India), and an adversary (China). British commentators sounded the alarm about Stuxnet as soon as the US role was apparent and warned that the worm signaled the start of a dangerous new era in competitive cyberattacks. Corera (2015a) wrote that unleashing Stuxnet was akin to crossing the digital Rubicon, and Lucas (2015) worried that the attack presaged a digital Pearl Harbor. In response, many argued that the best way forward was an open discussion about risks and efforts to create international norms that would constrain wanton cyberattacks. The risks of unintended consequences and collateral damage were perceived as too great to treat OCO as just another weapon. Writing in the *Financial Times*, Glenny (2012) predicted "we will rue Stuxnet's cavalier deployment." Writing in the *Guardian*, Chatterjee (2012) called for a "computer virus nonproliferation treaty" in order to prevent instances like Stuxnet. Therefore, the establishment of international norms became necessary.

British leaders, however, were more sanguine. While they increased investment in cyberdefenses, they also increased investment in OCO. Their attitude was that offensive cyberattacks were inevitable and they needed to prepare accordingly. Shortly after Stuxnet, the House of Commons Intelligence and Security Committee issued a report calling for better defenses and new offensive capabilities (Whitehead 2012). The defense secretary announced the creation of a new "cyber strike force" the following summer, and the military unveiled a new UK Joint Force Cyber Group to consolidate activities across services (Walters 2013; Corera 2015a). More recently, Chancellor George Osborne announced a new investment of £1.9 billion for defense OCO (Savage and Dean 2015). The initial fears of externalities caused by OCO seem to have had little effect on policymakers.

[14] Press releases downloaded from https://www.fbi.gov/collections/cyber. Dataset available from http://tylermoore.ens.utulsa.edu/FBIartco.xlsx.

There is also no evidence that London reduced cooperation with the United States. In the days after Stuxnet was revealed, British intelligence chief Jonathan Evans warned that "vulnerabilities in the Internet are being exploited by . . . states." Interestingly, he was referring to China and Russia and made no indication that he or any other official opposed the US operation (Financial Times 2012).[15] Later, Prime Minister David Cameron and President Obama announced a series of joint war-games specifically designed to test cyberdefenses and infrastructure security (Dean 2015).

The same pattern held in India, one of the states most affected by Stuxnet. While Iran was the intended target, thousands of Indian computers were likewise infected. Commentators sounded the alarm about what the attack meant for Indian cybersecurity. Citing a report that more than 80,000 computers were affected, one technology writer concluded that India was "caught in the crossfire" of a "global cyber war" that could lead to "massive collateral damage" (Anwer 2012). Nonetheless, Indian leaders did not express anger with the United States or reservations about continued cooperation with their American counterparts. Like the British, they saw Stuxnet as a useful warning about how future cyberattacks might threaten industrial systems and infrastructure and expressed concern that China in particular might exploit defensive gaps. They seemed resigned to a future in which cyberattacks are inevitable and moved to improve their capacity to both defend against them and to fight back.

Indeed, Stuxnet led to a flurry of activity designed to improve security and rationalize the use of OCO. The military created joint cybersecurity commands, the prime minister's office created the position of a national cybersecurity coordinator, the government stepped up efforts to recruit young hackers, and the Defense Intelligence Agency and National Technology Research Organization were given lead authority in exploring OCO (Joseph 2012; Bagchi 2012; Times of India 2013; Pandit 2013; Relia 2016).

The Chinese response was somewhat different. Like their counterparts in India and the UK, Chinese leaders saw Stuxnet as a wakeup call. Chinese infrastructure was particularly at risk because Chinese technology lagged behind the West (Li 2014). In July 2012, the state council released an update to its decade-old cybersecurity policy that emphasized China's glaring deficiencies compared to its rivals. It warned that the "broadband information infrastructure development gap with developed countries has widened; the level of government information sharing and business collaboration is not high; (and) the core technology is controlled by others" (Lindsay 2015, 12–13). Uncoordinated cybersecurity policies and weak infrastructure defenses exacerbated vulnerabilities to attacks like Stuxnet, and Chinese leaders were eager to resolve them quickly.

Initially, their response was similar to their reaction after the Persian Gulf War in 1991, when Chinese military leaders were awestruck and dismayed at US military technology and convinced they needed to emulate Washington's military "transformation" with their own modernization effort (Christensen 2001). The Chinese Communist Party (CCP) set up a small group of political leaders in February 2014 under President Xi Jinping, an indication of the importance with which the party viewed the issue. As Xi put it at the time, "there is no national security without internet security, and there is no modernization without informatization" (Li 2014; see also Segal 2014). China also began investing in academic research on cybersecurity to mitigate a series of technological and organizational problems (Li and Xu 2015). These steps are similar to the reaction among US allies and third parties. The possibility of cyberattack, they believe, is a fact to be reckoned with, and investment in better cybersecurity capabilities is the necessary response.

However, China went further. Beijing used the episode to emphasize what it calls "internet sovereignty" (Zheng 2015). According to Chinese leaders, responsible states have no choice but to patrol their virtual borders against malicious actors who spread disinformation or attack Chinese facilities via OCO. Modern states jealously guard their physical borders, they argue, so why should the internet be any different? Chinese leaders were quick to emphasize the need for better defenses given that Stuxnet disabled systems at a high security and air-gapped facility. Their responses also came at a time in which US leaders were more aggressively blaming China for cyberespionage against the United States. Cooperative efforts, like the US-China Cyber Working Group, were temporarily suspended (Gady 2016).

Although less information is currently available on the technical measures outlined above, the available data suggests resilience. The incident responses we can measure thus far do not indicate internet fragility. The distributed denial-of-service (DDoS) attacks launched on US banks by Iran in retaliation for Stuxnet steadily attenuated. The attacks, dubbed Operation Ababil, occurred in three distinct phases, and by the last phase, the attacks

[15] Critics of a deal to give a Chinese firm minority stake in a proposed nuclear power plant also warned that this might open the door to cyberattacks on Britain's energy infrastructure. Their fear was not technology, per se, but with specific adversaries (Macalister 2013).

were less frequent and easier for banks to manage (Schwartz 2013). Additionally, security firms have reported that the outage duration for DDoS attacks has fallen, and that the response times had improved the most for the financial sector. This was the area specifically targeted by Iran (Kitten 2015).

Research on data breaches has found that despite media claims, there is no evidence that the frequency of data breaches increased between 2005 and 2015, nor did the number of records breached increase during that time (Edwards, Hofmeyer, and Forrest 2015). Wheatley et al. (2016) draw similar conclusions about the relatively constant rate of data breach occurrence, though they do acknowledge that the magnitude may be increasing.

Infrastructure responses also indicate resilience. Encrypted web traffic spiked following the Snowden disclosures. By some estimates, it more than doubled (Finley 2014). Many popular websites changed their defaults so that incoming connections were encrypted over HTTPS, including Google and Facebook. Additionally, support for perfect forward secrecy (PFS) in HTTPS has skyrocketed. According to the SSL Pulse, in October 2013, 54 percent of popular websites tracked did not support PFS at all, 42 percent supported only some suites, and just 4 percent of websites were supported in browsers. By May 2016, only 20 percent lack any support and 54 percent of websites used forward security elements (FSE) by default in popular browsers (Trustworthy Internet Movement 2017).

Three broad conclusions flow from this analysis. First, Stuxnet did not change the behavior of most internet users, despite the fact that it affected many countries outside the intended target. Only one in ten users took steps to reduce exposure to government surveillance or otherwise reduce online activities. Notably, the number of users in this category is likely smaller than the number of first-time users since 2013. Second, firms responded by establishing their own programs to acquire vulnerability information for defensive purposes and continued to resist sharing cyberthreat information with governments as they had done prior to Stuxnet. This suggests that while firms were attuned to the events, they did not fundamentally change their behavior in the aftermath. Finally, states seem to have perceived the case as a cautionary tale about infrastructure vulnerabilities and subsequently invested in improving defenses. They also invested in more offensive capabilities, suggesting they are resigned to the possibility of cyberattacks in the future as a normal piece of contemporary international politics. In fact, they did not stop cooperating with the United States once implicated in Stuxnet, suggesting that the internet can flourish as an environment where complex attacks are possible, even expected, but not dismantling. China's move toward "internet sovereignty" challenges this view, but its policies may be less a consequence of Stuxnet than part of a larger story about an aspiring great power trying to increase its own influence and assert itself as an alternative to the US-led liberal order.

State responses after the Snowden revelations were more significant. The news made US officials appear hypocritical given that Washington was simultaneously pushing for norms governing acceptable conduct online. As one critic noted, "In light of the Snowden disclosures, the United States is poorly placed to persuade other actors of its good faith or its commitment to shared interests and values" (Farrell 2015). The combination of US power, its aggressive attempts to manipulate cyberspace, and its seeming hypocrisy all gave states good reason to turn inward.

Nonetheless, there is not much evidence that states stopped cooperating with US agencies on cybersecurity issues. Relations recovered quickly even in cases where the rhetorical gap was largest. Brazil, in particular, aims to be a leader in global internet governance and emphasizes multistakeholder models of internet governance that challenge traditional hierarchical organization. Such models favor an evolutionary approach that invites a wide array of actors to participate, often encouraging the utopian ideals of an open and apolitical domain unsullied by government restrictions. The accusation in July 2013 that the NSA had been collecting information on millions of Brazilians hit particularly hard. Brazil's senate announced an investigation of the United States and the foreign ministry announced it would work through the United Nations (UN) to "guarantee cybersecurity that protects the rights of citizens." (Segal 2016, p. 214) Things only got worse after further revelations that the NSA had intercepted President Dilma Rousseff's telephone calls and emails. Speaking at the UN, Rousseff accused the United States of violating international law and suggested its behavior hinted of authoritarianism (Segal 2016, 214). However, the acrimony was short-lived, and less than two years later, Rousseff travelled to Washington to meet with President Obama, where both pledged to resume cybersecurity cooperation (Obama and Rousseff 2015). This suggests that while intensive spying may have a short-term effect on political relations, even intense disputes do not undermine long-term internet security cooperation.

For China, Snowden's revelations may have broadened the appeal for internet sovereignty. Policymakers in Switzerland, South Korea, and elsewhere have spoken of the need to "de-Americanize" the internet (Segal 2016, 154). This does not mean the end of cooperation, but does suggest that other states see new reasons to reduce US influence over internet governance. This is akin to other policy domains where states are technologically interdependent, yet seek alternatives as a way of hedging reliance on great power partners. Small states rely on the United States for satellite imagery and signals intelligence, for instance, yet seek to cultivate their own sources and do not always cooperate fully with US overtures. In this regard, questions about cyberspace may be moving toward a more familiar brand of international relations in which autonomous states continually wrestle with one another for influence and autonomy, while simultaneously recognizing that for practical and technological reasons they cannot go it alone. As some observers predicted the return of politics long before Snowden, his actions have likely sped up the process (Mueller 2008).

Reactions to the Snowden disclosures mirrored broader political relations. On the one hand, close allies of the United States were more likely to defend the NSA than adversaries. British Prime Minister David Cameron castigated the *Guardian* for its role in disseminating Snowden's information, while simultaneously questioning the meaning of the leaks. Where some saw nefarious deeds, he saw something much more benign. As Cameron stated in January 2014, "I think the public reaction as I judge it has not been one of 'shock horror!' but one of 'intelligence agencies carry out intelligence work: good'" (Wintour 2014). On the other hand, allies with more difficult political relations, especially Germany, were not so charitable. And adversaries like China and Russia took an exceedingly dim view of the NSA, while simultaneously using the controversy to deflect attention from their own cyberactivities. Subsequently, the combined impact of Stuxnet and the Snowden revelations likely encouraged states to accelerate their own cybersecurity capabilities. Notably, though, there is little evidence that states have reduced cybersecurity cooperation, or that the short-term political damage from Snowden has led to the kind of Balkanization that could permanently cripple the internet.

Summary

We develop new measures for assessing whether or not the underlying technology is physically capable of absorbing cyberattacks, while focusing on the importance of political perceptions following cyberattacks in determining cybersecurity policy. Our measures of fragility show that while Stuxnet and Snowden have had important consequences, the system itself has proven resilient. Users have not lost enthusiasm for communicating online, despite repeated warnings about privacy violations and vulnerability to surveillance. The most important consequence seems to have been a small reduction in web searches for sensitive terms, though it is unclear whether the result lasted beyond the first few months after the scandal broke. And while firms have elected to pursue defenses on their own and have maintained a skeptical view toward cooperation with governments on cyberthreats, such strained relations predate the Stuxnet and Snowden controversies. Finally, while states have increased efforts to shore up their cybersecurity capabilities in the aftermath of Stuxnet and Snowden, they have not reduced cooperation on cybersecurity in general.[16]

Cybersecurity may have elements of a global public good, but this article demonstrates that scholars should be investigating rather than assuming that the maintenance of global public goods requires hegemonic leadership. The two cases we examine show cybersecurity to be resilient even when the hegemon is not playing by the rules. The policy implications are straightforward. The system appears resilient and self-sustaining even under stress. The expanse of the internet—a hodge-podge of state institutions, international coordinating bodies, and private firms—may make US control unworkable even if desirable. Such resiliency means, however, that United States efforts to protect its national security, even developing offensive tools for cyberspace, may not have the deleterious trade-offs on cybersecurity that HST would expect. A number of legal, political, and operational factors influence decisions regarding intelligence collection and OCOs. None of these factors should be taken lightly, and the preceding discussion is not meant to offer policymakers a green light for any and all cybersecurity policies. Our findings nonetheless suggest that policymakers should not be overly concerned that their actions will lead to significant harm to the internet.

References

Adams, Andrew A., Kiyoshi Murata, Yasunori Fukuta, Yohko Orito, and Ana María Lara Palma. 2015. "The View from the Gallery: International Comparison of Attitudes to Snowden's Revelations about the NSA/GCHQ." *ACM SIGCAS Computers and Society* 45 (3): 376–83.

Anderson, Ross, and Tyler Moore. 2006. "The Economics of Information Security." *Science* 314 (5799): 610–13.

[16] Although we have not had the time to test the case in detail, there also seems to have been only minor impacts from the alleged Russian hacking operation during the 2016 election. This suggests that the internet is resilient even if national and international politics are in turmoil.

Andrew, Christopher, and Vasili Mitrokhin. 1999. *The Sword and the Shield: The Mitrokhin Archive and the Secret History of the KGB*. New York, NY: Basic Books.

Anwer, Javed. 2012. "India Caught in Crossfire of Global Cyber War." *Times of India*, August 20. http://www.gadgetsnow.com/it-services/India-caught-in-crossfire-of-global-cyber-war/articleshow/15567180.cms.

Avey, Paul C., Jonathan N. Markowitz, and Robert J. Reardon. 2017. "Disentangling Grand Strategy: The Promise and Perils of Grand Theory" (working paper).

Bagchi, Indani. 2012. "NSA Bids to Intensify Cyber-Security System." *Times of India*, August 9. http://timesofindia.indiatimes.com/india/NSA-bids-to-intensify-cyber-security-system/articleshow/15412231.cms.

Chatterjee, Pratap. 2012. "The Urgency of a Computer Virus Nonproliferation Treaty." *Guardian*, June 27. https://www.theguardian.com/commentisfree/2012/jun/27/urgency-computer-virus-nonproliferation-treaty.

Christensen, Thomas J. 2001. "Posing Problems without Catching Up: China's Rise and Challenges for U.S. Security Policy." *International Security* 25 (4): 5–40.

Chucri, Nazli. 2012. *Cyberpolitics in International Relations*. Cambridge, MA: MIT Press.

Corera, Gordon. 2015. *Intercept: The Secret History of Computers and Spies*. London: Weidenfeld and Nicolson.

—— 2015a. "We're Hopelessly Behind Our Enemies in Cyberwar." *Times of London*, July 11. http://www.thetimes.co.uk/article/were-hopelessly-behind-our-enemies-in-cyberwar-x7p7wtnqww9.

Dean, James. 2015. "We Don't Know How to Stop Cyberterror, Security Boss Admits." *Times of London*, February 2. http://www.thetimes.co.uk/article/we-dont-know-how-to-stop-cyberterror-security-boss-admits-q6h25xwsx8z.

US Department of Homeland Security. "Cybersecurity Insurance Workshop Readout Report." Last modified November 2012, accessed 2015. https://www.dhs.gov/sites/default/files/publications/November%202012%20Cybersecurity%20Insurance%20Workshop.pdf

Drezner, Daniel W. 2013. "Military Primacy Doesn't Pay (Nearly as Much as You Think)." *International Security* 38 (1): 52–79.

Edwards, Benjamin, Steven Hofmeyer, and Stephanie Forrest. 2015. "Hype and Heavy Tails: A Closer Look at Data Breaches." *Journal of Cybersecurity* 2 (1): 2016.

Espiner, Tom. 2012. "British Stuxnet Could Have Unintended Fallout, Government Admits." *ZDnet*, July 18. http://www.zdnet.com/article/british-stuxnet-could-have-unintended-fallout-government-admits/.

Falliere, Nicolas, Liam O. Murchu, and Eric Chien. 2011. *W32.Stuxnet Dossier*, version 1.4. Cupertino, CA: Symantec Security Response. https://www.symantec.com/content/en/us/enterprise/media/security_response/whitepapers/w32_stuxnet_dossier.pdf.

Farrell, Henry. 2015. *"Promoting Norms in Cyberspace: a Cyber Brief."* New York: Council on Foreign Relations.

Financial Times. 2012. "Telling the Truth about Cyberwarfare," June 26. https://www.ft.com/content/777fe5ae-bf86-11e1-a476-00144feabdc0.

Finley, Klint. 2014. "Encrypted Web Traffic More than Doubles after NSA Revelations." *Wired*, May 16. https://www.wired.com/2014/05/sandvine-report/.

Gady, Franz-Stefan. 2016. "What Does 2016 Hold for U.S.-China Relations in Cyberspace?" *Diplomat*, January 29. http://thediplomat.com/2016/01/what-does-2016-hold-for-china-us-relations-in-cyberspace/.

Government Accountability Office. "Critical Infrastructure Protection: Key Private and Public Cyber Expectations Need to Be Consistently Addressed." Last modified August 16, 2010, accessed 2015. http://www.gao.gov/products/GAO-10-628.

Gholz, Eugene, and Daryl G. Press. 2010. "Protecting 'the Prize': Oil and the U.S. National Interest." *Security Studies* 19 (3): 453–85.

Gilpin, Robert. 1981. *War and Change in World Politics*. Cambridge, MA: Cambridge University Press.

—— 1987. *The Political Economy of International Relations*. Princeton, NJ: Princeton University Press.

Glenny, Misha. 2012. "We Will Rue Stuxnet's Cavalier Deployment." *Financial Times*, June 6. https://www.ft.com/content/6b674600-afc7-11e1-a025-00144feabdc0.

Google. "Google Vulnerability Reward Program (VRP) Rules." Google Application Security, accessed 2015. https://www.google.com/about/appsecurity/reward-program/.

Gowa, Joanne. 1989. "Rational Hegemons, Excludable Goods, and Small Groups: An Epitaph for Hegemonic Stability Theory?" *World Politics* 41 (3): 307–24.

Greenwald, Glenn. 2013. "NSA collecting phone records of millions of Verizon customers daily." *Guardian*, June 6. https://www.theguardian.com/world/2013/jun/06/nsa-phone-records-verizon-court-order.

Gunasekara, Gahan, Kiyoshi Murata, Andrew A. Adams, and Ana María Lara Palma. 2015. "Young People Do Care: Snowden's Revelations Have Had an Effect in New Zealand." *ACM SIGCAS Computers and Society* 45 (3): 369–75.

International Atomic Energy Agency (IEAE). "Implementation of the NPT Safeguards Agreement and Relevant Provisions of Security Council Resolutions in the Islamic Republic of Iran." Paper deristricted at the IEAE Board of Governors meeting, June 5, 2013. https://www.iaea.org/sites/default/files/gov2013-27.pdf.

Ikenberry, G. John. 1998–99. "Institutions, Strategic Restraint, and the Persistence of American Postwar Order." *International Security* 23 (3): 43–78.

—— 2000. *After Victory: Institutions, Strategic Restraint, and the Rebuilding of Order after Major Wars*. Princeton, NJ: Princeton University Press.

Joseph, Josy. 2012. "India to Add Muscle to Its Cyber Arsenal." *Times of India*, June 11. http://timesofindia.indiatimes.com/india/India-to-add-muscle-to-its-cyber-arsenal/articleshow/14004730.cms.

Keohane, Robert O. 1984. *After Hegemony: Cooperation and Discord in the World Political Economy*. Princeton, NJ: Princeton University Press.

Kim, Eugene. 2015. "Companies Are Freaked Out About Cybersecurity And Plan To Spend A Lot More On It This Year." *Business Insider*, January 6. http://www.businessinsider.com/

piper-jaffray-survey-shows-companies-spending-more-on-cyber-security-2015-1.

Kindleberger, Charles. 1973. *The World in Depression: 1929–1939*. Berkeley: University of California Press.

Kitten, Tracy. 2015. "DDoS Attacks Against Banks Increasing: Financial Institutions Seek New Ways to Mitigate the Risks." *Bank Info Security*, August 24. http://www.bankinfosecurity.com/ddos-a-8497.

Landale, Jeff, and Sascha Meinrath. 2015. "Opinion: The Troubling Stuxnet Effect." *Christian Science Monitor*, November 4. http://www.csmonitor.com/World/Passcode/Passcode-Voices/2015/1104/Opinion-The-troubling-Stuxnet-effect.

Levi, Michael. 2013. "The Enduring Vulnerabilities of Oil Markets." *Security Studies* 21 (3): 132–38.

Li, Jing. 2014. "Cybersecurity Chief Warns of 'Ideological Penetration." *South China Morning Post*, May 19. http://www.lexisnexis.com/lnacui2api/api/version1/getDocCui?lni=5C7B-BVV1-JC8V-13TW&csi=270944,270077,11059,8411&hl=t&hv=t&hnsd=f&hns=t&hgn=t&oc=00240&perma=true.

Li, Yuxiao, and Li. Xu 2015. "China's Cybersecurity Situation and the Potential for International Cooperation." In *China and Cybersecurity: Espionage, Strategy, and Politics in the Digital Domain*, edited by Jon R. Lindsay, Tai Ming Cheung and Derek S. Reveron, 225–241. New York: Oxford University Press.

Lindsay, Jon R. 2013. "Stuxnet and the Limits of Cyber Warfare." *Security Studies* 22 (3): 365–404.

—— 2015. "Introduction - China and Cybersecurity: Controversy and Context." In *China and Cybersecurity: Espionage, Strategy, and Politics in the Digital Domain*, edited by Jon R. Lindsay, Tai Ming Cheung, and Derek S. Reveron, 1–27. New York: Oxford University Press.

Lucas, Edward. 2015. *Cyberphobia: Identity, Trust, Security, and the Internet*. London: Bloomsbury.

Macalister, Terry. 2013. "UK Energy Infrastructure 'At Risk of Shutdown from Cyberattacks." *Guardian*, October 18. https://www.theguardian.com/business/2013/oct/18/uk-energy-infrastructure-risk-cyber-attacks.

Madaan, Neha. 2012. "Few Net Users Know About Online Threats." *Times of India*, September 13. http://timesofindia.indiatimes.com/city/pune/Few-net-users-aware-about-online-threats/articleshow/16382896.cms?.

Matthews, Alex and Catherine Tucker. 2015. "Government Surveillance and Internet Search Behavior." Working paper currently under review. https://www.sebastianwendt.de/wp-content/uploads/2015/06/Government-Surveillance-and-Internet-Sea.

McElwee, Sean, Matt McDermott, and Will Jordan. 2017. "4 pieces of evidence showing FBI Director James Comey cost Hillary Clinton the election." *Vox*, January 11 http://www.vox.com/the-big-idea/2017/1/11/14215930/comey-email-election-clinton-campaign.

McKeown, Timothy J. 1983. "Hegemonic Stability Theory and 19th Century Tariff Levels in Europe." *International Organization* 37 (1): 73–91.

McPherson, Steven H. and Glenn Zimmerman. 2010. "Cyberspace Control." In *Securing Freedom in the Global Commons*, edited by Scott Jasper, 83–98. Stanford, CA: Stanford University Press.

Moore, Tyler, Scott Dynes, and Frederick Chang. "Identifying how firms manage cybersecurity investment." Paper presented at the 15th Annual Workshop on the Economics of Information Security (WEIS), Berkeley, CA, June 2016.

Mueller, Milton. 2008. "Securing Internet Freedom: Security, Privacy, and Global Governance." Inaugural address of Professor Dr. Milton Mueller, XS4All Professor, Technology University of Delft, Information and Communication Technology section, Faculty of Technology, Policy and Management, Delft, Netherlands, October 17. http://faculty.ischool.syr.edu/mueller/opzet1.pdf.

Mulligan, Deirdre K., and Fred B. Schneider. 2011. "Doctrine for Cybersecurity." *Dædalus* 140 (4): 70–92.

Obama, Barack, and Dilma Roussef. 2015. "Joint Communiqué by President Barack Obama and President Dilma Rousseff." *The White House, Office of the Press Secretary*, June 30. https://obamawhitehouse.archives.gov/the-press-office/2015/06/30/joint-communique-president-barack-obama-and-president-dilma-rousseff.

Oliva, Mario Arias, Ana María Lara Palma, Kiyoshi Murata, and Andrew A. Adams. 2015. "Information Surveillance by Governments: Impacts of Snowden's Revelations in Spain." *ACM SIGCAS Computers and Society* 45 (3): 398–406.

Oxford Economics. 2011. *The New Digital Economy: How it Will Transform Business*. Oxford: Oxford Economics. https://www.ciaonet.org/attachments/18539/uploads.

Pandit, Rajat. 2013. "Tri-Service Commands for Space, Cyber Warfare." *Times of India*, May 18. http://timesofindia.indiatimes.com/india/Tri-service-commands-for-space-cyber-warfare/articleshow/20115462.cms.

Powell, Benjamin. 2005. "Is Cybersecurity a Public Good? Evidence from the Financial Services Industry." *Journal of Law, Economics, and Policy* 1 (2): 497–510.

Rainie, Lee, and Mary Madden. 2015. "Americans' Privacy Strategies Post-Snowden." *Pew Research Center*, March 16. http://www.pewinternet.org/2015/03/16/americans-privacy-strategies-post-snowden/.

Raymond, Mark. 2013. "Puncturing the Myth of the Internet as a Commons." *Georgetown Journal of International Affairs* 13: 57–68.

Relia, Sanjeev. 2016. *Cyber Warfare: Its Implications for National Security*. Delhi: Vij Books India.

Rosenzweig, Paul. 2011. "Cybersecurity and Public Goods: The Public/Private 'Partnership.'" In *Emerging Threats in National Security and Law*, edited by Peter Berkowitz. http://media.hoover.org/sites/default/files/documents/EmergingThreats_Rosenzweig.pdf.

Ross, Robert S. 1999. "The Geography of the Peace: East Asia in the Twenty-First Century." *International Security* 23 (4): 81–118.

Rovner, Joshua, and Caitlin Talmadge. 2014. "Hegemony, ForcePosture, and the Provision of Public Goods: The Once and Future Role of Outside Powers in Securing Persian Gulf Oil." *Security Studies* 23 (3): 548–81.

Savage, Michael, and James Dean. 2015. “£1.9bn for cyber-attacks on terrorists.” *Times of London*, November 18. http://www.thetimes.co.uk/article/pound19bn-for-cyberattacks-on-terrorists-22glsxw2bmj.

Schneier, Bruce. 2015. *Data and Goliath: The Hidden Battles to Collect Your Data and Control Your World*. New York: W.W. Norton.

Schwartz, Matthew. 2013. “Bank Attackers Restart Operation Ababil DDoS Disruptions.” *Dark Reading*, March 6. http://www.darkreading.com/attacks-and-breaches/bank-attackers-restart-operation-ababil-ddos-disruptions/d/d-id/1108955.

Segal, Adam. 2014. “China’s New Small Leading Group on Cybersecurity and Internet Management.” *Council on Foreign Relations*, February 27. http://blogs.cfr.org/asia/2014/02/27/chinas-new-small-leading-group-on-cybersecurity-and-internet-management/.

—— 2016. *The Hacked World Order: How Nations Fight, Trade, Maneuver, and Manipulate in the Digital Age Author*. New York: Public Affairs.

Sheetz, Mark S. 1997–98. “Debating the Unipolar Moment.” *International Security* 22 (3): 168–75.

Singer, P.W., and Allan Friedman. 2014. *Cybersecurity and Cyberwar: What Everyone Needs to Know*. Oxford: Oxford University Press.

Skierka, Isabel, Robert Morgus, Mirko Hohmann, and Tim Maurer. “CSIRT Basics for Policy Makers: The History, Types & Culture of Computer Security Incident Response Teams.” New America Foundation Working Paper, 2015. https://na-production.s3.amazonaws.com/documents/CSIRT_Basics_for_Policy-Makers_May_2015_WEB_09-15.16efa7bcc9e54fe299ba3447a5b7d41e.pdf.

Snidal, Duncan. 1985. “The Limits of Hegemonic Stability.” *World Politics* 39 (4): 579–614.

Statista. “Number of internet users worldwide from 2005 to 2015.” Last modified 2015. Accessed March 2016. http://www.statista.com/statistics/273018/number-of-internet-users-worldwide/

Times of India. 2013. “TCS ex-CEO Ramadorai: Time to Hire Ethical Hackers.” *Times of India*, October 14. http://www.lexisnexis.com/lnacui2api/api/version1/getDocCui?lni=59K3-3XP1-DXJR-H4F9&csi=270944,270077,11059,8411&hl=t&hv=t&hnsd=f&hns=t&hgn=t&oc=00240&perma=true.

Trustworthy Internet Movement. “SSL Pulse: Survey of the SSL Implementation of the Most Popular Web Sites,” last modified May 3, 2017, accessed May 29, 2016. https://www.trustworthyinternet.org/ssl-pulse/.

US Census Bureau. 2015. E-commerce Statistics. https://www.census.gov/newsroom/press-releases/2017/cb17-tps48.html.

Valeriano, Brandon, and Ryan C. Maness. 2015. *Cyber Warfare versus Cyber Realities: Cyber Conflict in the International System*. Oxford: Oxford University Press.

Walters, Simon. 2013. “Hammond’s £500m New Cyber Army.” *Mail on Sunday*, September 28. http://www.dailymail.co.uk/news/article-2436946/Hammonds-500m-new-cyber-army-As-reveals-secret-Whitehall-bunker-time-Defence-Secretary-says-future-wars-fought-viruses.html.

Waltz, Kenneth N. 1979. *Theory of International Politics*. New York: McGraw Hill.

Wheatley, Spencer, Thomas Maillart, and Didier Sornette. 2016. “The extreme risk of personal data breaches and the erosion of privacy.” *The European Physical Journal B* 89 (7): 1–12.

Whitehead, Tom. 2012. “Destroy our Cyber Enemies, say MPs.” *Daily Telegraph*, July 17. http://www.telegraph.co.uk/news/uknews/law-and-order/9399014/Destroy-our-cyber-enemies-say-MPs.html.

Wintour, Patrick. 2014. “Cameron Says He Failed to Make Case for Mass Surveillance After Snowden Leaks.” *Guardian*, January 30. https://www.theguardian.com/politics/2014/jan/30/cameron-failed-mass-surveillance-snowden-communication-laws.

Yetiv, Steve A. 2015. *Myths of the Oil Boom: American National Security in a Global Energy Market*. Oxford: Oxford University Press.

Zetter, Kim. 2011. “How Digital Detectives Deciphered Stuxnet, the Most Menacing Malware in History.” *Wired*, July 11. https://www.wired.com/2011/07/how-digital-detectives-deciphered-stuxnet/.

—— 2014. *Countdown to Zero Day: Stuxnet and the Launch of the World’s First Digital Weapon*. New York: Crown Publishing.

Zheng, Ye. 2015. “From Cyberwarfare to Cybersecurity in the Asia-Pacific and Beyond.” In *China and Cybersecurity: Espionage, Strategy, and Politics in the Digital Domain*, edited by Jon R. Lindsay, Tai Ming Cheung, and Derek S. Reveron, 123–37. New York: Oxford University Press.