Cybersecurity Norm-Building and Signaling with China

Geoffrey Hoffman

Cite as: Hoffman, Geoffrey. 2020. “Cybersecurity Norm-Building and Signaling with China.” In *Governing Cyberspace: Behavior, Power, and Diplomacy*, edited by Dennis Broeders and Bibi van den Berg,187-204. London: Rowman & Littlefield International.

More information about the book and The Hague Program for Cyber Norms is available on:

www.thehaguecybernorms.nl

Chapter 9

Cybersecurity Norm-Building and Signaling with China

Geoffrey Hoffman

In the endeavor to establish global cybersecurity norms, China's Internet censorship presents an obstacle for democracies. China, with over 800 million Internet users (CINIC 2018), is the largest and least free entity on the Internet (Freedom House 2017), but democracies often couple cybersecurity norms with Internet freedom. Nevertheless, China and democracies share an objective to improve global cybersecurity cooperation in order to make the Internet a safer place—both from each other and from the other myriad hostile actors—and establishing norms is a primary means of attaining this end (Finnemore and Hollis 2016, 436). Using the Operation Aurora cyber espionage campaign as a case study, the hypothesis emerges that cybersecurity norm-building between democracies and China is more likely to succeed when democracies decouple cybersecurity from Internet freedom, and that signaling can address some of the difficulties inherent in this decoupling.

It can be challenging to define cybersecurity norms: many norms already exist, many of those norms dovetail, and multiple lower-level norms may, together, construct a single, higher-level norm. Martha Finnemore and Duncan B. Hollis (2016, 426–427) point out that, while "calls for 'cybernorms' to secure and govern cyberspace are now ubiquitous," cybersecurity is actually "a diverse array of problems." Yet, they further contend that much of the power of norms "lies in the processes by which they form and evolve" (Finnemore and Hollis 2016, 427). Aurora provides a novel context in which to examine this process. Further, the concept of decoupling here refers to democracies working with China to establish mutually beneficial cybersecurity norms that are wholly independent from Internet freedom—the 2015 Obama-Xi cybersecurity pact is one example (Sanger 2016).

Early idealists had hoped that the Internet, by virtue of the unfettered access it provided to information, would act as a force of liberal reform in

authoritarian states—and, indeed, it might have, had the Internet remained free and open (Hwang 2018). Instead, China, via the Great Firewall, retooled its domestic Internet into the world's largest censorship apparatus and, despite the efforts of the United States and other democracies, further tightens its Internet controls every year (*Bloomberg News* 2017). China's refusal to adopt domestic or international liberal norms for the Internet presages that the cybersecurity norms among democracies will be different from those between democracies and China—and from those between China and other authoritarian states. Indeed, China has already demonstrated this difference in norms by signing a cybersecurity pact with Russia based on sharing Great Firewall technology (*The Guardian* 2016), and by selling censorship technology to Iran (Stecklow 2012). In other words, while democracies are building cybersecurity norms coupled with Internet freedom, authoritarian states are building cybersecurity norms coupled with Internet censorship. The common bridge between the two sets is cybersecurity, alone.

Margaret Roberts (2018, 37) defines censorship as "the restriction of the public expression of or public access to information by authority when the information is thought to have the capacity to undermine the authority by making it unaccountable to the public." Democracies engage in censorship to different degrees; the flooding of misinformation during the last US election, for instance, has spurred debate on the culpability of Internet companies and whether they should censor their users (Reynolds 2018). However, democracies generally have laws defending free speech (Roberts 2018, 15–16), whereas China argues for its sovereign right to censor. China's government tells private companies, directly, what to censor (Zhuang 2018). Lu Wei, the former head of the Cyberspace Administration of China, said, "I, indeed, may choose who comes into my house. They can come if they are friends," and, "Freedom is our goal. Order is our means" (Martina 2015). Thus, censorship is a nuanced concept, and contrasting democracies as having Internet freedom with China as having Internet censorship is a porous abstraction. Nevertheless, for a broad look at cybersecurity norm-building, this abstraction is useful—with the caveat that, as a complex issue, its purpose is to underscore the fundamental difference that democracies seek the best approach to information freedom, whereas China seeks greater information control.

There are three barriers to decoupling cybersecurity from Internet freedom. The first barrier is that democracies view Internet freedom as a human right while China does not, which compels democracies to pressure China on Internet censorship. Article 19 of the Universal Declaration of Human Rights (1948) recognizes freedom of opinion and expression as a human right, and Internet freedom is that right on the Internet. One cybersecurity expert illustrates the resistance to decoupling cybersecurity from Internet freedom by criticizing the 2015 Obama-Xi cybersecurity pact: "There is nothing in this

agreement that addresses Chinese censorship or abuse of human rights. While some might argue that those are not issues related to hacking, a government that shuts off access to portions of the Internet that allow free communication is essentially no different than a party that executes denial-of-service attacks. And human rights cannot be left off the table" (Steinberg 2015).

The second barrier is that cybersecurity and Internet freedom are operationally entangled. To varying degrees, democracies engage in open or collaborative cybersecurity, while China uses censorship as a cybersecurity tool. From the US Department of Defense's bug bounty programs (Newman 2017) to NATO's (2018) collective cyber defense in which "allies are committed to enhancing information-sharing and mutual assistance in preventing, mitigating and recovering from cyber attacks," Internet freedom is an important part of the liberal approach to cybersecurity. On the other hand, China uses the Great Firewall's censorship capabilities for cybersecurity; for instance, China used the Great Firewall to crack down on anonymity tools like Virtual Private Networks (VPNs) (Lin and Kubota 2018)—which hackers can use to hide their location. Conversely, China also uses cybersecurity for censorship purposes; for example, one analyst argues that a cybersecurity regulation that permits both local and central authorities to search the offices of Internet service providers is "designed to more effectively implement China's censorship directives" (Gan 2018).

The final barrier is the moral question of whether this decoupling should occur. Do the benefits of greater Internet peace and security outweigh the risks of further censorship normalization that might arise from cooperative cybersecurity efforts with China? That is, even if democracies can overcome the first two barriers to cybersecurity norm-building with China, it is not clear that they should. However, both governments and technology companies have signaled that this decoupling is already occurring: from the tenuous bilateral cybersecurity pacts China has signed with the United States and a number of other democracies that make no mention of censorship (Burgess 2017) to Apple removing censorship-evading apps from its App Store in China and Google's leaked plans to reintroduce a censored version of its search engine in China (Doubek 2018).

Robert Jervis (1989, 18) defines signals as "statements or actions . . . issued mainly to influence the receiver's image of the sender." In order for signals to be credible, they must be costly—this cost establishes the sender's commitment to the signal. During Aurora, most of the costly signaling that occurred was the *ex post*, tying-hands type—commitments that would result in audience costs if abandoned (Fearon 1997). Simply put, if an actor adopts a stance but does not follow through, they suffer reputation loss. James D. Morrow (1999, 86) writes, "In international politics, signaling is a way to consider the problem of unknown motivation." Signaling, then, is an important tool in the

U.S.-China diplomatic toolbox because it helps to frame the norm formation and evolution process.

China has been signaling that it was open to cybersecurity norm-building at least since the release of its white paper *The Internet in China* in 2010, which called for multilateral cooperation to combat "the increasingly serious problem of transnational network crimes" (IOSCPRC 2010). This white paper was a by-product of an early clash of incompatible cybersecurity norms: Google and the US conflict with China over the Aurora cyber espionage campaign. Using this clash as a case study, it appears that signaling offers an answer to the first two barriers to decoupling. Specifically, signaling can allow cybersecurity norms to cultivate in a separate channel from Internet freedom pressures, and it can help identify and extricate the elements of cybersecurity bound to Internet freedom or censorship.

THE OPERATION AURORA ATTACKS: BACKGROUND

Google has had a difficult relationship with China beyond the inherent market challenges (Madden 2010). It entered China in January 2006 with google.cn, a censored version of its search engine (*CNN* 2006). A Google statement explained its calculus: "While removing search results is inconsistent with Google's mission, providing no information (or a heavily degraded user experience that amounts to no information) is more inconsistent with our mission" (Crampton 2006). Although Google said it would report to users when information was removed from search results (*CNN* 2006), there was, nevertheless, a widespread belief that google.cn violated the company's "don't be evil" policy (*BBN News* 2006). For instance, the following month, a congressional subcommittee on human rights summoned Google—along with other Internet companies—to defend their "sickening collaboration," as the subcommittee chairman put it, with the Chinese government (Zeller 2006).

Google's founders struggled with the choice. Sergey Brin, who claimed that his childhood in the authoritarian Soviet Union influenced his views on censorship (Lohr 2010), spent a year with Larry Page weighing the decision to censor on their "evil scale" (Walker 2010). Reflecting on it a year later, he said, "On a business level, that decision to censor . . . was a net negative" (Martinson 2007). He also remarked that the company had suffered because of the damage to its reputation in the United States and Europe (Martinson 2007). However, he eventually defended the moral reasoning behind google.cn, believing that it was the best decision for the Chinese people (McManus 2010).

In 2010, Google and the US government clashed with the Chinese government over cybersecurity norms. There were two central issues: China's Aurora cyber espionage campaign and China's Internet censorship (Lau

2010). Although not the first—nor most recent—Chinese cyber espionage campaign against the United States (Denning 2017), Aurora's high degree of politicization was unique. As a result, government signaling played a new and interesting role in the cybersecurity norm-building process.

The clash began in January 2010, when Google announced the discovery of a cyberattack, originating in China, that stole its intellectual property and also targeted at least twenty other businesses (Drummond 2010a). Google also noted that "a primary goal of the attackers was accessing the Gmail accounts of Chinese human rights activists" and that, as a consequence, Google would no longer censor google.cn for China (Drummond 2010a). Later that day, in an official statement, US secretary of state Hillary Clinton (2010b) expressed concern over Google's allegations and sought an explanation from China. She also announced that she would be giving a speech on Internet freedom.

Clinton delivered her speech, "Remarks on Internet Freedom," nine days later. It was a *tour de force* on the virtues of Internet freedom and cooperation. She argued that the Internet—as "a new nervous system for our planet"—when free and open, was an unprecedented force for good for individuals, societies, governments, and businesses, but that it could also be repurposed for oppression—and authoritarian regimes were using it this way through censorship. This censorship, she contended, contravened the United Nations Universal Declaration of Human Rights (Clinton 2010a).

At its core, Clinton's speech called for the establishment of global Internet freedom and cybersecurity norms, which she coupled together. She stated, "New technologies do not take sides in the struggle for freedom and progress, but the United States does. We stand for a single Internet where all of humanity has equal access to knowledge and ideas. And we recognize that the world's information infrastructure will become what we and others make of it." Tying this theme to cybersecurity, she remarked that online commerce and intellectual property "are all at stake if we cannot rely on the security of our information networks," that "disruptions in these systems demand a coordinated response by all governments, the private sector, and the international community," and, further, that "we have taken steps as a government, and as a Department, to find diplomatic solutions to strengthen global cyber security." She also announced that the US Department of State would support the development of new circumvention technologies to help evade Internet censorship (Clinton 2010a).

The broader issue, Clinton explained, is "whether we live on a planet with one internet, one global community, and a common body of knowledge that benefits and unites us all, or a fragmented planet in which access to information and opportunity is dependent on where you live and the whims of censors. Information freedom supports the peace and security that provides a

foundation for global progress." She made a point of speaking directly to the private sector, arguing that "censorship should not be in any way accepted by any company from anywhere. And in America, American companies need to make a principled stand. This needs to be part of our national brand. I'm confident that consumers worldwide will reward companies that follow those principles" (Clinton 2010a).

Unsurprisingly, she also addressed the Chinese government, asking it to conduct a thorough and transparent investigation into Google's allegations. She noted that, while the United States and China had different views on Internet censorship, they should "address those differences candidly and consistently in the context of our positive, cooperative, and comprehensive relationship." She further warned of censorship's implications for international peace and security: "Historically, asymmetrical access to information is one of the leading causes of interstate conflict. When we face serious disputes or dangerous incidents, it's critical that people on both sides of the problem have access to the same set of facts and opinions" (Clinton 2010a).

In short, Google and the United States were arguing that China's Internet censorship was a human rights violation. China, however, countered that Google needed to obey its laws if it wished to operate there (Fletcher 2010a). In agreement with China was J. Stapleton Roy, a former US ambassador to China, who said, "I don't understand their calculation. I do not see how Google could have concluded that they could have faced down the Chinese on a domestic censorship issue" (Wong 2010). Also siding with China were Microsoft Corporation's Steve Ballmer (2010), who said "we are all subject to local laws," and Bill Gates, who said, "You've got to decide: do you want to obey the laws of the countries you're in or not? If not, you may not end up doing business there" (Johnson and Branigan 2010).

Furthermore, it is important to note that it is unclear whether human rights or, in fact, economics was the deeper motivation for the coordinated Google and US response to Aurora. Not doing well in China despite censoring its search engine, Google's best business decision may have been to improve its international reputation by sacrificing its China operations for a noble cause (Lacy 2010). Similarly, the United States was eager to push back against China's recurring cyber espionage efforts (Metzl 2011). From this perspective, the issue of human rights served as convenient pressure point to achieve other goals.

THE OPERATION AURORA ATTACKS: TIMELINE

Following Jervis's (1989) definition of signals, the methodology for recognizing signals is to identify, from the narrative of this clash, statements, or

actions that were intended to alter another actor's perception. Thus, a timeline of the Aurora conflict follows.

January

On January 12, 2010, Google revealed the Aurora cyber espionage campaign to the public, beginning the escalation with the Chinese government (Drummond 2010a). Google announced that they, along with a wide range of other businesses, had been hacked (Drummond 2010a). Google claimed that the target was both its intellectual property and the e-mail accounts of human rights activists, and that the attacks originated in China (Drummond 2010a). Later that day, Clinton (2010b) made her statement seeking an explanation from the Chinese government. Google and Clinton implied that the Chinese government was responsible but had not explicitly assigned blame.

Two days later, a Chinese Foreign Ministry spokeswoman said that Chinese law prohibits any form of hacking attacks and she emphasized that foreign companies needed to respect Chinese law (Fletcher 2010a). She declined, however, to answer a question about whether the illegality of hacking extended to government hacking (Fletcher 2010a). That same day, security researchers at Verisign declared that the Chinese government was behind the attack, claiming that "the government of China has been engaged for months in a massive campaign of industrial espionage against U.S. companies" (Paul 2010). Security researchers at McAfee also investigated the attack, naming it "Operation 'Aurora' " (Goodin 2010a).

On January 18, Google began an investigation into its Chinese employees (Branigan 2010), and, the next day, it postponed the launch of two Android mobile phones in China (Lee and Buckley 2010). On January 21, Clinton (2010a) gave her speech on Internet freedom. The following day, China rebuffed Clinton, warning that her words were dangerous to U.S.–China relations (Fletcher 2010b). At the World Economic Forum at Davos, Google CEO Eric Schmidt remarked, "We like what China is doing in terms of growth . . . we just don't like censorship. We hope that will change and we can apply some pressure to make things better for the Chinese people" (Blumenstein and Fidler 2010).

February

Google began coordinating with the US National Security Agency to analyze the attacks, with the objective to better defend against future attacks (Nakashima 2010). On February 10, evidence emerged that the attacks were still ongoing and had targeted many more companies than Google originally estimated (Higgins 2010). On February 12, Brin said that, given the size

of the Chinese government, it was not important whether it was behind the attacks (Zetter 2010). He also remarked that Google was hopeful that it could remain in China and was willing to permit some types of censorship, such as for adult content and gambling, but not political censorship (Zetter 2010). On February 17, the cybersecurity company iSEC published a report detailing the difficulty of defending against Aurora and claimed that it had actually targeted over one hundred companies. The next day, investigators linked Aurora to two Chinese universities (Goodin 2010b). On February 23, for the first time, the Chinese government officially rejected Google's allegations (Graham-Harrison 2010).

March

The United States then considered taking the issue of China's forcing censorship on Google to the WTO as an unfair trade barrier (Drajem 2010). On March 12, China's chief Internet regulator insisted Google must obey its laws or "pay the consequences" (Pomfret 2010). The state-run news agency Xinhua attacked Google's "intricate ties with the U.S. government" on March 21 (*BBC News* 2010*)*. The following day, Google ended its google.cn censorship and tested a new strategy of automatically redirecting visitors from google.cn to google.com.hk, whose servers were located in Hong Kong and so not subject to the mainland's censorship laws (Drummond 2010b). In response, an official in China's State Council Information Office said that Google's move was "totally wrong" and "violated its written promise" (Metz 2010). As a result, on March 23, the Chinese government attempted to restrict the mainland's access to Google's Hong Kong-based servers (Metz 2010).

April–November

On April 20, referencing Article 19 of the Universal Declaration on Human Rights, Google launched a new worldwide tool that displayed the number of government requests for user data or content removal (Drummond 2010d). The Chinese government, on June 8, released the white paper *The Internet in China* defending its Internet policies (Bristow 2010). On June 28, Google announced that the Chinese government would not accept its redirect solution and would deny the renewal of its business license (Drummond 2010c). Consequently, Google attempted a new strategy, turning google.cn into a static webpage that only contained a link to their uncensored Hong Kong-based site, rather than forcing an automatic redirect (Drummond 2010c). Google stated, "This new approach is consistent with our commitment not to self censor and, we believe, with local law (Drummond 2010c)." The new strategy worked: on July 9, Google's China business license was renewed (Drummond 2010c).

From that point on, both sides remained relatively peaceable, even after a WikiLeaks cable, released on November 28, implicated the Chinese Politburo in the Aurora attacks (Shane and Lehren 2010).

THE OPERATION AURORA ATTACKS: SIGNALS

During Aurora, there were roughly four groups of tying-hands signals that used reputation as an audience cost. The first signal of significance occurs at the beginning of the conflict: Google revealing Aurora to the public and tying its hands by announcing the plan to end its censorship. To the international community and to its users, Google signaled a recommitment to its "don't be evil" policy. To the Chinese government, it signaled that there were both physical and virtual consequences to China's hostile actions in cyberspace. These potential consequences included Google no longer abiding China's censorship laws—possibly even leaving China—and China suffering international reputation loss.

The second signal was the response of the US government. Google and the US Department of State may have coordinated the initial public response to occur on the same day for greater impact. From this viewpoint, it was a two-pronged act of Thomas Schelling's (1966, 69) concept of compellence, with the threat being that the United States would escalate the issue in Clinton's upcoming speech if China did not justify itself before then. China did not, and, with Clinton's speech and the later threat to take the matter to the WTO, the United States signaled that it would respond in both the physical and virtual spheres to actions that harm its interests in cyberspace. Broadly, the United States was tying its hands to a willingness to escalate matters.

The third set of signals was the cumulative reaction of the Chinese government. There were four important individual responses: first, the response two days after the first statements by Google and Clinton; second, the response the day after Clinton's address on Internet freedom; third, the response after more evidence had accumulated linking the Chinese government to the attacks, and finally, the publication of *The Internet in China*, the Chinese government's white paper defending its Internet practices. Each response added something: the first, that foreign companies must follow China's domestic laws; the second, that what was best for the Chinese people was China's concern, and so Clinton's comments were damaging to U.S.–China relations; and the third, that Google's allegations in its January 12 statement were "groundless," stating that "China administers its Internet according to law, and this position will not change. China prohibits hacking and will crack down on hacking according to law" (Graham-Harrison 2010). This was the first time China had directly refuted the allegations, over five weeks after Aurora came to light.

China's fourth response, the white paper *The Internet in China*, both reiterated and expanded on the messages of the first three responses. Like Clinton's speech, it expressed the importance of international cooperation on cybersecurity. The white paper was both China's version of and ultimate response to the speech, and it was an argument for China's Internet sovereignty within its borders. Interestingly, apparently in response to Clinton's call for Internet freedom, it claimed that the Chinese government "guarantees the citizens' freedom of speech on the Internet as well as the public's right to know, to participate, to be heard and to oversee in accordance with the law" (IOSCPRC 2010). China was tying its hands to the argument that both the United States and China permit Internet freedom in accordance with law, but that those laws were different.

The final signals occurred during rapprochement. Because Google and the United States confronted China publicly, China had to respond in a way that would mitigate its international reputation loss. By emphasizing the illegality of hacking and making the issue of censorship a matter of legal compliance, China was able to defend its requirements for renewing Google's business license. By permitting Google to adhere to the letter of the law but not the spirit, China signaled that, even in sensitive areas like censorship, legal compliance had some flexibility.

The silence that followed the renewal of Google's business license—silence that even the new WikiLeaks evidence did not interrupt—signaled that both sides were eager to move forward from the clash. China and Google continued their tenuous relationship, although China never fully relented: it slowed down and intermittently disrupted Google's services—a form of censorship (Roberts 2018, 42)—finally blocking google.com.hk altogether in 2014 (Levin 2014). Nevertheless, at the time, Google was able to offer a link to an uncensored search engine for users who sought it, and China was satisfied that Google capitulated to its regulations. In the end, however, all three actors suffered some reputation loss: evidence had implicated the government of China in the attack, the international community remembered that Google had "spent four years, and earned vast sums of money, operating under China's censorship laws" (Carr 2010), and Clinton's appeal for global Internet freedom had achieved little.

DECOUPLING CYBERSECURITY AND INTERNET FREEDOM

Despite working in conjunction, it is clear that Google's efforts in the Aurora conflict were relatively successful, while the United States' efforts were not. To wit, although Google was struggling in a hostile market environment and

the victim of cyber espionage, Google's public retaliation eventually resulted in the renewal of its business license without continuing to censor its search engine. On the other hand, as powerful as Clinton's speech and the following WTO threat were, the United States did not succeed in compelling China to lessen its information controls, in preventing businesses from becoming increasingly interdependent with China, or in yielding from China a transparent investigation into Aurora or an admission of wrongdoing. Nor did it substantially lessen China's cyber espionage efforts against the United States (Denning 2017). Thus, Google's actions serve as the better model: Google received and responded to China's signals and made more progress. It is important to consider two points, however: first, that without the accompanying pressure from the United States, China might not have been as willing to accept Google's solution; and second, Google's business interests are minor in scope in comparison to the US foreign policy interests.

From the beginning, China signaled that Google could stay by obeying China's laws. Google found it could obey these laws by rerouting traffic to its uncensored Hong Kong site, first testing China's limits with an automatic redirect before retreating to a link that required manual effort. Simultaneously, Google increased its pressure on China to reduce censorship by adding a reporting tool for government censorship requests—but it added this tool separately from its effort to renew its business license. Thus, Google overcame the first barrier—that Internet freedom is a human right—to decoupling cybersecurity from Internet freedom. Google funneled pressure against censorship through a different channel—an unrelated reporting tool, in this case—while cultivating a cybersecurity norm of following China's laws and expecting, in return, a more secure operating environment. Google achieved this favorable outcome despite its "don't be evil" policy and Brin's personal enmity toward censorship.

Through its white paper, China signaled that it desired to cooperate on cybersecurity relating to "transnational network crimes," but also that its cyber sovereignty commitment was uncompromising (IOSCPRC 2010). Clinton signaled a similar intransigence on cybersecurity cooperation, stipulating Internet freedom as an elemental component. The United States made its appeal to the international community for Internet freedom, its ambitions to create anti-censorship tools, and its threat to take the matter to the WTO in conjunction with the appeal for global cybersecurity norm-building. If the United States had separated these efforts, as it did during the later Obama-Xi summit, it might have made more progress in overcoming the first barrier.

Google's success, however, illustrates how signaling can help democracies pressure China on censorship separately from cybersecurity norm-building; it suggests that democracies can decouple the two without giving up on Internet freedom. Google's experience also demonstrated the second barrier—that

cybersecurity and Internet freedom are operationally entangled—by working with the US government and international security researchers on analyzing Aurora. China had, in its white paper, stated that different states have different needs for Internet cooperation: "Though connected, the Internet of various countries belongs to different sovereignties, which makes it necessary to strengthen international exchanges and cooperation in this field" (IOSCPRC 2010). In other words, it signaled that cybersecurity norm-building requires calibrating the norms to those differences. In Google's case, the expectation of not being the target of government-sponsored cyber espionage was not contingent on having Internet freedom in China. That is, while Google could not expect full operational freedom in China, it could still seek to build a norm of operational cybersecurity.

China, by proclaiming that hacking was illegal—despite that it, itself, was doing the hacking—signaled that this concept served as a foundation to build on, and Google accepted the signal by seeking ways to continue its China operations. The secure business environment that China signaled was a norm-building effort operationally disentangled from Internet freedom or censorship. Perhaps to validate the honesty of this signal, Aurora eventually did stop. In contrast, Clinton's speech operationally coupled Internet freedom with cybersecurity, implying that improving global cybersecurity would only be possible alongside Internet freedom, and so it did not overcome the second barrier. Google's relative progress here suggests that signaling can offer insights into operational disentanglement.

The final barrier to decoupling cybersecurity from Internet freedom is the moral component. Even if democracies can decouple the two for norm-building with China, should they? Although this question will endure, a couple points worthy of consideration stand out. The fact that cybersecurity norm-building is separable from Internet freedom goals, without preventing efforts to achieve those goals, is an argument in favor. On the other hand, these efforts might be weaker, overall, and so further entrench China's censorship practices. The condemnation from human rights groups over the recent capitulations of US companies to China's censorship demands illustrates this concern (Doubek 2018).

In the Aurora conflict, China offered valuable information through signaling. Although signals can be dishonest (Jervis 1989, 18), China's renewal of Google's business license, after Google responded to China's signals, demonstrated honesty. Google used these signals to decouple Internet freedom—without abandoning it—from cybersecurity norm-building with China, as well as to discern the operational requirements of such norms. Conversely, the United States showed that not decoupling the two is a dead end. Thus, the hypothesis emerges that cybersecurity norm-building between democracies and China is more likely to succeed if cybersecurity is not coupled with

Internet freedom, and that signaling can help overcome two of the barriers to this decoupling.

Interestingly, the literature on signaling has argued that authoritarian regimes are less effective than democracies at sending tying-hands signals with *ex post* costs because the domestic audience costs are lower or obfuscated (Weiss 2013, 1–2). Jessica Chen Weiss (2013, 2) shows that authoritarian states can employ nationalist, anti-foreign protests as a substitute for the way democracies use official statements as tying-hands signals. Yet, during Aurora, China's official statements appeared to be honest signals. The first possibility is that the signals were costless but happened to be honest anyway. The second possibility, which seems more likely, is that the costs were not domestic but rather from the international audience. The world was watching, and if China had backed down from its stance of being in the legal right, the international political and business community's perception of China would adjust accordingly.

Although China's authoritarianism might intrinsically restrict the bandwidth of potential cybersecurity cooperation, something changed in democracies' willingness to seek it in the time between Clinton's speech on Internet freedom in 2010 and 2015 Obama-Xi cybersecurity summit. The summit occurred while the US Department of State was funding the development of censorship evasion tools, and the resulting pact, which temporarily succeeded in reducing the frequency of Chinese cyberattacks on the United States (Sanger 2016), made no mention of censorship (Brown and Yung 2017). The pact, along with China's other cybersecurity pacts in recent years, overcame the three barriers to decoupling and may suggest that democracies are becoming more receptive to the idea. As cybersecurity becomes more important to international security, democracies may increasingly view cybersecurity norms as independent from others.

BIBLIOGRAPHY

Ballmer, Steve. 2010. "Microsoft & Internet Freedom." Official Microsoft Blog, Microsoft. January 27, 2010. https://blogs.microsoft.com/blog/2010/01/27/microsoft-internet-freedom/.

Blumenstein, Rebecca and Stephen Fidler. 2010. "Google Takes Aim at Beijing Censorship." *Wall Street Journal*, January 30, 2010. https://www.wsj.com/articles/SB10001424052748703389004575033100778834196.

Branigan, Tania. 2010. "Google Investigates China Staff Over Cyber Attack." *Guardian*, January 18, 2010. https://www.theguardian.com/technology/2010/jan/18/china-google-cyber-attack.

Bristow, Michael. 2010. "China Defends Internet Censorship." *BBC News*, June 8, 2010. http://news.bbc.co.uk/2/hi/americas/8727647.stm.

Brown, Gary and Christopher D. Yung. 2017. "Evaluating the US-China Cybersecurity Agreement, Part 1: The US Approach to Cyberspace." *Diplomat*, January 19, 2017. https://thediplomat.com/2017/01/evaluating-the-us-china-cybersecurity-agreement-part-1-the-us-approach-to-cyberspace/.

Burgess, Christopher. 2017. "Dissecting China's Global Bilateral Cybersecurity Strategy." *Security Boulevard*, October 9, 2017. https://securityboulevard.com/2017/10/dissecting-chinas-global-bilateral-cybersecurity-strategy/.

Carr, Paul. 2010. "Soul Searching: Google's Position on China Might Be Many Things, But Moral It Is Not." *TechCrunch*, January 13, 2010. https://techcrunch.com/2010/01/13/not-safe-for-wok/.

"China Denounces Google 'US ties.'" *BBC News*, March 21, 2010. http://news.bbc.co.uk/2/hi/asia-pacific/8578968.stm.

China Internet Network Information Center. 2018. "第42次《中国互联网络发展状况统计报告》发布." August 20, 2018. https://cnnic.net.cn/gywm/xwzx/rdxw/20172017_7047/201808/t20180820_70486.htm.

Clinton, Hillary. 2010a. "Remarks on Internet Freedom." U.S. Department of State. January 21, 2010. https://2009-2017.state.gov/secretary/20092013clinton/rm/2010/01/135519.htm.

Clinton, Hillary. 2010b. "Statement on Google Operations in China." U.S. Department of State. January 12, 2010. https://2009-2017.state.gov/secretary/20092013clinton/rm/2010/01/135105.htm.

Crampton, Thomas. 2006. "Google Puts Muzzle on Itself in China." *New York Times*, January 24, 2006. https://www.nytimes.com/2006/01/24/technology/google-puts-muzzle-on-itself-in-china.html.

Denning, Dorothy. 2017. "How the Chinese Cyberthreat Has Evolved." *Conversation*, October 4, 2017. https://theconversation.com/how-the-chinese-cyberthreat-has-evolved-82469.

Doubek, James. 2018. "Google Testing a Censored Search Engine Just for China." *NPR*, August 2, 2018. https://www.npr.org/2018/08/02/634827587/google-testing-a-censored-search-engine-just-for-china.

Drajem, Mark. 2010. "Google Wants U.S. to Weigh Challenging China in WTO." *Bloomberg*, March 3, 2010. https://www.bloomberg.com/news/articles/2010-03-03/google-wants-u-s-to-weigh-challenging-china-in-wto.

Drummond, David. 2010a. "A New Approach to China." *Official Blog*, Google. January 12, 2010. https://googleblog.blogspot.com/2010/01/new-approach-to-china.html.

Drummond, David. 2010b. "A New Approach to China: An Update." *Official Blog, Google*. March 22, 2010. https://googleblog.blogspot.com/2010/03/new-approach-to-china-update.html.

Drummond, David. 2010c. "An Update on China." *Official Blog, Google*. July 9, 2010. https://googleblog.blogspot.com/2010/06/update-on-china.html.

Drummond, David. 2010d. "Greater Transparency Around Government Requests." *Official Blog, Google*. April 20, 2010. https://googleblog.blogspot.com/2010/04/greater-transparency-around-government.html.

Fearon, James D. 1997. "Signaling Foreign Policy Interests: Tying Hands versus Sinking Costs." *The Journal of Conflict Resolution*. 41, no. 1 (February): 68–90. http://www.jstor.org/stable/174487.

Finnemore, Martha and Duncan B. Hollis. 2016. "Constructing Norms for Global Cybersecurity." *American Journal of International Law*. 110, no. 3 (July): 425–479. https://doi.org/10.1017/S0002930000016894.

Fletcher, Owen. 2010a. "China Emphasizes Laws as Google Defies Censorship." *PCWorld*, January 14, 2010. https://www.pcworld.com/article/186881/article.html.

Fletcher, Owen. 2010b. "China slams Clinton's Call for Internet Freedom." *Computerworld*, January 22, 2010. https://www.computerworld.com/article/2523071/enterprise-applications/china-slams-clinton-s-call-for-internet-freedom.html.

"Freedom on the Net 2017." Freedom House, November 2017. https://freedomhouse.org/report/freedom-net/freedom-net-2017.

Gan, Nectar. 2018. "Chinese Police Get Power to Inspect Internet Service Providers." *South China Morning Post*. October 6, 2018. https://www.scmp.com/news/china/politics/article/2167240/chinese-police-get-power-inspect-internet-service-providers.

Goodin, Dan. 2010a. "IE Zero-Day Used in Chinese Cyber Assault on 34 Firms." *Register*, January 14, 2010. https://www.theregister.co.uk/2010/01/14/cyber_assault_followup/.

Goodin, Dan. 2010b. "Most Resistance to 'Aurora' Hack Attacks Futile, Says Report." *Register*, March 1, 2010. https://www.theregister.co.uk/2010/03/01/aurora_resistence_futile/.

"Google move 'black day' for China." *BBC News*, January 25, 2006. http://news.bbc.co.uk/2/hi/technology/4647398.stm.

"Google to Censor Itself in China." *CNN*, January 26, 2006. http://www.cnn.com/2006/BUSINESS/01/25/google.china/.

Graham-Harrison, Emma. 2010. "China Says Google Hacking Claims 'groundless.'" *Reuters*, February 23, 2010. https://www.reuters.com/article/us-china-google/china-says-google-hacking-claims-groundless-idUSTRE61M2FM20100223.

Higgins, Kelly Jackson. 2010. "'Aurora' Attacks Still Under Way, Investigators Closing In On Malware Creators." *Darkreading*, February 10, 2010. https://www.darkreading.com/attacks-breaches/aurora-attacks-still-under-way-investigators-closing-in-on-malware-creators/d/d-id/1132922.

Hwang, Tim. 2018. "The Four Ways That Ex-Internet Idealists Explain Where It All Went Wrong." *MIT Technology Review*, August 22, 2018. https://www.technologyreview.com/s/611805/the-four-ways-that-ex-internet-idealists-explain-where-it-all-went-wrong.

IOSCPRC (Information Office of the State Council of the People's Republic of China). 2010. *The Internet in China*. June 8, 2010. http://www.china.org.cn/government/whitepaper/node_7093508.htm.

Jervis, Robert. 1989. *The Logic of Images in International Relations*. New York: Columbia University Press.

Johnson, Bobbie and Tania Branigan. 2010. "Web Censorship in China? Not a Problem, Says Bill Gates." *Guardian*, January 25, 2010. https://www.theguardian.com/technology/2010/jan/25/bill-gates-web-censorship-china.

Lacy, Sarah. 2010. "Google's China Stance: More About Business Than Thwarting Evil." *TechCrunch*, January 12, 2010. https://techcrunch.com/2010/01/12/google's-china-stance-more-about-business-than-thwarting-evil/.

Lau, Justine. 2010. "A History of Google in China." *Financial Times*, July 9, 2010. http://ig-legacy.ft.com/content/faf86fbc-0009-11df-8626-00144feabdc0#axzz5PhJFzwqh.

Lee, Melanie and Chris Buckley. 2010. "Google Postpones Cellphone Launch in China." *Reuters*, January 19, 2010. https://www.reuters.com/article/idINIndia-45511720100119.

Levin, Dan. 2014. "China Escalating Attack on Google." *New York Times*, June 2, 2014. https://www.nytimes.com/2014/06/03/business/chinas-battle-against-google-heats-up.html.

Lin, Liza and Yoko Kubota. 2018. "China's VPN Crackdown May Aid Government Surveillance." *Wall Street Journal*. January 17, 2018. https://www.wsj.com/articles/chinas-vpn-crackdown-may-aid-government-surveillance-1516189155.

Lohr, Steve. 2010. "Interview: Sergey Brin on Google's China Move." *New York Times*, March 22, 2010. https://bits.blogs.nytimes.com/2010/03/22/interview-sergey-brin-on-googles-china-gambit/.

Madden, Normandy. 2010. "Google Isn't the Only Silicon Valley Company Struggling in China." *Business Insider*, January 19, 2010. https://www.businessinsider.com/google-isnt-the-only-silicon-valley-company-struggling-in-china-2010-1.

Markoff, John and David Barboza. 2010. "2 China Schools Said to Be Tied to Online Attacks." *New York Times*, February 18, 2010. https://www.nytimes.com/2010/02/19/technology/19china.html.

Martina, Michael. 2015. "China's Cyber Chief Defends Censorship Ahead of Internet Conference." *Reuters*, December 9, 2015. https://www.reuters.com/article/us-china-internet/chinas-cyber-chief-defends-censorship-ahead-of-internet-conference-idUSKBN0TS0X720151209.

Martinson, Jane. 2007. "China Censorship Damaged Us, Google Founders Admit." *Guardian*, January 27, 2007. https://www.theguardian.com/technology/2007/jan/27/news.newmedia.

McManus, Emily. 2010. "Sergey Brin on Google's China Decision." TEDBlog, TED. February 24, 2010. https://blog.ted.com/our_focus_has_b/.

Metz, Cade. 2010. "China Hits Back at Google's Uncensored Hong Kong Servers." *Register*, March 23, 2010. https://www.theregister.co.uk/2010/03/23/china_moves_to_restrict_google_hong_kong_services/.

Metzl, Jamie. 2011. "China and Cyber-Espionage." *HuffPost*, October 22, 2011. https://www.huffingtonpost.com/jamie-metzl/china-and-cyberespionage_b_931918.html.

Morrow, James D. 1999. "The Strategic Setting of Choices: Signaling, Commitment, and Negotiation in International Politics." In *Strategic Choice and International Relations*, edited by David A. Lake and Robert Powell, 77–114. Princeton: Princeton University Press.

Nakashima, Ellen. 2010. "Google to Enlist NSA to Help It Ward Off Cyberattacks." *Washington Post*, February 4, 2010. http://www.washingtonpost.com/wp-dyn/content/article/2010/02/03/AR2010020304057.html.

Newman, Lily Hay. 2017. "The Pentagon Opened Up to Hackers—And Fixed Thousands of Bugs." *Wired*, November 10, 2017. https://www.wired.com/story/hack-the-pentagon-bug-bounty-results/.

NATO (North Atlantic Treaty Organization). 2018. "Cyber Defense." July 16, 2018. https://www.nato.int/cps/en/natohq/topics_78170.htm.

Paul, Ryan. 2010. "Researchers Identify Command Servers Behind Google Attack." *Ars Technica*, January 14, 2010. https://arstechnica.com/information-technology/2010/01/researchers-identify-command-servers-behind-google-attack/.

Pomfret, John. 2010. "China Holds Firm Against Google, Says Firm Must Obey Its Laws." *Washington Post*, March 13, 2010. http://www.washingtonpost.com/wp-dyn/content/article/2010/03/12/AR2010031203564.html.

"Putin Brings China's Great Firewall to Russia in Cybersecurity Pact." *The Guardian*, November 29, 2016. https://www.theguardian.com/world/2016/nov/29/putin-china-internet-great-firewall-russia-cybersecurity-pact.

"Quicktake: The Great Firewall of China." *Bloomberg News*, November 30, 2017. https://www.bloomberg.com/quicktake/great-firewall-of-china.

Reynolds, Glenn Harlan. 2018. "When Digital Platforms Become Censors." *Wall Street Journal*, August 18, 2018. https://www.wsj.com/articles/when-digital-platforms-become-censors-1534514122.

Roberts, Margaret E. 2018. *Censored: Distraction and Diversion Inside China's Great Firewall*. Princeton: Princeton University Press.

Sanger, David E. 2016. "Chinese Curb Cyberattacks on U.S. Interests, Report Finds." *New York Times*, June 20, 2016. https://www.nytimes.com/2016/06/21/us/politics/china-us-cyber-spying.html.

Schelling, Thomas. 1966. *Arms and Influence*. Fredericksburg: BookCrafters.

Shane, Scott and Andrew W. Lehren. 2010. "Leaked Cables Offer Raw Look at U.S. Diplomacy." *New York Times*, November 28, 2010. https://www.nytimes.com/2010/11/29/world/29cables.html.

Stecklow, Steve. 2012. "Special Report: Chinese Firm Helps Iran Spy on Citizens." *Reuters*, March 22, 2012. https://www.reuters.com/article/us-iran-telecoms/special-report-chinese-firm-helps-iran-spy-on-citizens-idUSBRE82L0B820120322.

Steinberg, Joseph. 2015. "10 Issues With the China-US Cybersecurity Agreement." *Inc.*, September 27, 2015. https://www.inc.com/joseph-steinberg/why-the-china-us-cybersecurity-agreement-will-fail.html.

UN General Assembly. 1948. *Universal Declaration of Human Rights*. December 10, 1948, 217 A (III). http://www.un.org/en/universal-declaration-human-rights/.

Walker, Tim. 2010. "Sergey Brin: Engine Driver." *Independent*, January 16, 2010. https://www.independent.co.uk/news/people/profiles/sergey-brin-engine-driver-1869546.html.

Weiss, Jessica Chen. 2013. "Authoritarian Signaling, Mass Audiences, and Nationalist Protest in China." *International Organization*. 67, no. 1 (January): 1-35. http://journals.cambridge.org/abstract_S0020818312000380.

Wong, Edward. 2010. "Google Faces Fallout as China Reacts to Site Shift." *New York Times*, March 23, 2010. https://www.nytimes.com/2010/03/24/technology/24google.html.

Zeller, Tom, Jr. 2006. "Web Firms Are Grilled on Dealings in China." *New York Times*, February 16, 2006. https://www.nytimes.com/2006/02/16/technology/web-firms-are-grilled-on-dealings-in-china.html.

Zetter, Kim. 2010. "TED 2010: Google Optimistic It Can Remain in China." *Wired*, February 12, 2010. https://www.wired.com/epicenter/2010/02/ted-2010-google-optimistic-it-can-remain-in-china/.

Zhuang, Pinghui. 2018. "Weibo Falls Foul of China's Internet Watchdog for Failing to Censor Content." *South China Morning Post*, January 29, 2018. https://www.scmp.com/news/china/policies-politics/article/2130931/weibo-falls-foul-chinas-internet-watchdog-failing.

Governing Cyberspace

OPEN ACCESS

The publication of this book is made possible by a grant from the Open Access Fund of the Universiteit Leiden.