COUNCIL *on*
FOREIGN
RELATIONS

CYBER BRIEF

Promoting Norms for Cyberspace

Henry Farrell

April 2015

This Cyber Brief is part of the Digital and Cyberspace Policy program.

The United States defined its preferred cyberspace norms—Internet openness, security, liberty, free speech, and with minimal government oversight and surveillance—in its 2011 International Strategy for Cyberspace. Although the United States has had little success so far in establishing norms against commercial espionage in cyberspace, it has had some early gains with the recognition that international law applies to state activity in cyberspace and that human rights protections that apply offline also apply online.

These efforts to define shared norms have been accompanied by a process of norm promotion that suffered a significant setback in the summer of 2013 with the Snowden disclosures. The U.S. government should reinvigorate its efforts to spread and encourage the adoption of its preferred norms with the following steps:

- reform U.S. intelligence activities to make them more consistent with the publicly expressed norms of Internet openness that the United States is trying to establish;
- disclose more convincing evidence when trying to shame actors that do not abide by cybersecurity norms; and
- encourage other states and civil society actors to take a leading role in norm promotion—even when this cuts against U.S. interests.

BACKGROUND: WHY NORMS?

U.S. policymakers argue that the United States and others need to build norms to mitigate cybersecurity problems. Admiral Michael S. Rogers, head of the National Security Agency (NSA) and Cyber Command, has argued that shared norms are a basic building block for cybersecurity. He has called on actors in academia and civil society to help design them and to assist in their spread.

It may seem strange that Pentagon officials are arguing for soft tools rather than hard military options, but there are four good reasons why norms are the best option available. First, the United States is vulnerable to cyberattacks and this weakness is difficult to address using conventional tools of military statecraft. Second, it is difficult to ensure that complex information systems are fully defended, since they may have subtle technical weaknesses. Third, classical deterrence is not easy in a world where it is often challenging to identify sophisticated attackers, or even to know when an attack has taken place. Lastly, treaties are hard to enforce because it is so difficult to verify compliance—particularly in cyberspace, where weapons are software, not missiles.

Although norms are hazier than treaty rules, they may still have important consequences. Norms against the use of nuclear weapons have taken hold since the 1950s, making their use nearly unthinkable in ordinary circumstances. Robust cybersecurity norms might, over time, rule out some kinds of attacks as normatively inappropriate. They might encourage other states to see norm breaches as attacks on their security, too, spurring cooperation to prevent or stop attacks. Finally, norms can provide shared understandings between states that allow them to work together where they have shared interests and manage relations where their interests clash.

CHALLENGES TO NORM PROMOTION

It is hard to spread norms, even in the best circumstances. Unfortunately, these are far from the best circumstances for the United States. U.S. policymakers face three major problems. First, it is easiest to promote norms when one can invoke common values to support them, yet the world's cyber powers have different—and radically incompatible—values over how to protect cyberspace. The clashing interests between democratic and authoritarian regimes on the value of an open Internet and definitions of security make effective global treaties impossible.

Second, the potential adopters of norms are likely to be more receptive if they do not think the proponent of the norms is acting in bad faith. To be sure, many states were happy to use the Snowden revelations as a cover for opposition to any rules of behavior Washington might offer. But for others, efforts at persuasion have been damaged by the exposed gap between U.S. rhetoric and actions. At the very least, other states must be persuaded that following a norm is in their national interest. The disclosures, however, reinforced the view of many states that the United States disproportionately benefits from an open, global, and secure Internet, and is only committed to these values to the extent that they further U.S. economic, political, and military objectives.

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. The extent of the damage to the U.S. reputation was revealed when the United States accused North Korea of hacking into Sony's servers and announced its intention to retaliate against North Korea through low-level sanctions. Building on previous indictments of Chinese soldiers for hacking into U.S. firms, U.S. officials followed an approach of "naming and shaming" cyberattackers while pursuing sanctions and possible criminal charges. These actions are highly unlikely to result in successful prosecutions, but potentially serve a normative purpose by signaling to the world that some actions are unacceptable. Although a few states criticized North Korea, many did not buy U.S. claims that Pyongyang was responsible. Members of the business and technology communities also expressed polite skepticism over the evidence supplied by the Federal Bureau of Investigation.

Third, states are not the only important actors shaping norms on cyberspace. Sometimes they are not even the most significant players. Large e-commerce firms (which are tacitly reshaping norms around privacy and security by rebuilding the everyday architecture of cyberspace), and activists and experts (who both design and implement Internet protocols) play important and visible roles in shaping arguments about cyberspace policy. The U.S. government had been able to work in tacit—albeit sometimes uneasy—alliance with businesses, which favored minimum government interference across the globe, and with activists, who wanted to limit government surveillance and trusted the United States a little more than they trusted other countries. The Snowden disclosures shattered these unspoken alliances by revealing that the United States was secretly authorizing massive surveillance and undermining core cryptographic standards at the same time that it was advocating for a free and open Internet.

RECOMMENDATIONS

If the United States is serious about promoting a normative approach to interactions in cyberspace, it will have to undertake some difficult reforms. First, the NSA, the Central Intelligence Agency, and Cyber Command should adopt a fundamental change of mind-set, abandoning what legal scholar Margo Schlanger calls "intelligence legalism." Most U.S. intelligence officials pride themselves on obeying the law, but their understanding of the law sometimes depends on strained and secret interpretations that push the envelope of what is possible. As argued in President Barack Obama's Review Group on Intelligence and Communications Technologies, the review process for signal collection must be more clearly weighed against the potential damage to the normative commitments to an open and secure Internet held by the United States, its allies, and those whom the United States wishes to persuade. If the NSA wants to help develop strong norms, it will have to limit its own freedom to carry out operations that contravene the norms that the United States seeks to establish.

Second, if the U.S. government wishes to use naming and shaming tactics to develop norms, it will need evidence to support its claims. Shaming tactics face their own version of the attribution problem and the Snowden affair makes the U.S. government less inclined to share sensitive information, while some parts of the technical community are more likely to question the veracity of the information and less willing to cooperate. One possible way forward might be to develop an informal panel of independent technical experts from the global community of Computer Emergency Response Teams. The panel could convene on an ad hoc basis to review the evidence provided by a victim state, and the accused state could provide information to refute the victim's claim. Although it will be difficult to review highly sensitive information using such a loose arrangement, it should be possible to share some forensic data with these experts, allowing them to evaluate the veracity of claims. In some instances, governments may have to be willing to lose highly valued intelligence operations if they want their shaming tactics to be effective.

Third, to develop legitimate norms, the United States should let some of its partners take the lead. New norms will not be seen as legitimate if they are perceived to be solely a projection of U.S. interests. The Netherlands, for instance, has been active in promoting free expression on the Internet, and is hosting a Global Conference on Cyberspace in April 2015. A number of private groups and companies—the Global Network Initiative, Electronic Frontier Foundation (EFF), the Center for Democracy and Technology, and Microsoft—are working on norms of state behavior. The United States can exercise influence over norms, helping to convene initial groups, and perhaps imprinting the early process of debate with some of its core values. However, norms will only develop full legitimacy if they are associated with independent structures that evaluate them, debate them, and assess whether different actors are living up to them.

For the same reason, the United States should participate in systematic conversations with countries, businesses, and leading experts in the hope of generating some shared values that might lead to stronger normative commitments. This already happens through track-two diplomacy with China and other world powers. Paradoxically, it may be harder for the United States to start talking to the technology companies and groups like the EFF who share a common normative vocabulary of commitment to openness and free debate. The bitterness of the last two years will be difficult to overcome.

Implementing these three recommendations will require the U.S. government to change critical aspects of its approach to cybersecurity, balancing offensive and defensive strategies against the capacity to persuade. The U.S. government should identify ways to work with actors with whom it lacks mutual trust, in order to build legitimacy for its claims about appropriate actions in cyberspace. Finally, the government should support these much-needed conversations about norm building, while letting business and civil society actors take the lead. If the United States can carry through on these steps, it will be in a much better place to promote norms and, in the process, restore its own credibility.

About the Author

Henry Farrell is associate professor of political science and international affairs at George Washington University. He works on a variety of topics, including trust, the politics of the Internet, and international and comparative political economy. He has written articles and book chapters as well as a book, *The Political Economy of Trust: Interests, Institutions and Inter-Firm Cooperation*, published by Cambridge University Press.

The Council on Foreign Relations (CFR) is an independent, nonpartisan membership organization, think tank, and publisher dedicated to being a resource for its members, government officials, business executives, journalists, educators and students, civic and religious leaders, and other interested citizens in order to help them better understand the world and the foreign policy choices facing the United States and other countries. Founded in 1921, CFR carries out its mission by maintaining a diverse membership, with special programs to promote interest and develop expertise in the next generation of foreign policy leaders; convening meetings at its headquarters in New York and in Washington, DC, and other cities where senior government officials, members of Congress, global leaders, and prominent thinkers come together with CFR members to discuss and debate major international issues; supporting a Studies Program that fosters independent research, enabling CFR scholars to produce articles, reports, and books and hold roundtables that analyze foreign policy issues and make concrete policy recommendations; publishing *Foreign Affairs*, the preeminent journal on international affairs and U.S. foreign policy; sponsoring Independent Task Forces that produce reports with both findings and policy prescriptions on the most important foreign policy topics; and providing up-to-date information and analysis about world events and American foreign policy on its website, CFR.org.

The Council on Foreign Relations takes no institutional positions on policy issues and has no affiliation with the U.S. government. All views expressed in its publications and on its website are the sole responsibility of the author or authors.

The Digital and Cyberspace Policy program addresses one of the twenty-first century's most pressing challenges: keeping the global Internet open and secure in the face of unprecedented threats. Through briefings, reports, and the *Net Politics* blog, the program's fellows produce timely analysis on the most important issues in cyberspace. Cyber Briefs are short memos that offer concrete recommendations on cybersecurity, Internet governance, online privacy, and the trade of digital goods and services.

For further information about CFR or this paper, please write to the Council on Foreign Relations, 58 East 68th Street, New York, NY 10065, or call Communications at 212.434.9888. Visit CFR's website, www.cfr.org.