COUNCIL on FOREIGN RELATIONS

CYBER BRIEF

Maintaining U.S. Leadership on Internet Governance

Megan Stifel
February 2017

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

After almost two decades of overseeing the internet naming and addressing system, the U.S. government transferred the responsibility to a coalition of industry, civil society, and government stakeholders in October 2016. The United States relinquished its role to demonstrate to emerging countries its commitment to significant private sector involvement in the operation of the internet. The move had overwhelming support from industry and like-minded governments, but some policymakers, including Donald J. Trump when he was running for office, saw the announcement as an ill-considered loss of direct control over the most important communications medium ever developed. Given that the transition is effectively irreversible, the United States needs to respond to new institutional and political realities and find alternative ways to maintain its influence on internet governance. The U.S. government should do this by collaborating with industry to enhance the internet's reliability and resilience by tackling vulnerabilities that permit foreign governments to question the current governance approach. Additionally, it should expand efforts to foster and train leaders in emerging internet markets.

BACKGROUND

A collection of technical actions, known as the Internet Assigned Numbers Authority (IANA) functions, ensures that the internet works. The U.S. government sought to privatize the IANA functions by 2000, hoping to streamline and keep accountable the hodgepodge of U.S.-funded research agreements, individuals, and companies that were responsible for them. However, the government missed its deadline and a U.S. government agency, the National Telecommunications and Information Administration (NTIA), contracted with the Internet Corporation for Assigned Names and Numbers (ICANN) for the execution of the IANA functions. The contract led some to believe that the U.S. government controlled the internet.

That perception has become a lightning rod of controversy, dividing opinion on internet governance into two groups. The first group, led by Western governments and the private sector, argues that the internet should be governed through a multistakeholder approach, involving self-identified stakeholders such as businesses, public interest groups, technical experts, and governments in a consensus-based decision-making process. The other group, led by Russia and China, proposes an intergovernmental approach to managing the internet, in which national governments would be the chief rule makers online. The drawbacks to an intergovernmental approach have been described elsewhere: stagnant innovation, restricted speech, and reduced interoperability, to name a few. Although the United States has always supported the multistakeholder approach, its failure to fully transition the IANA functions undermined its promotion efforts and fueled arguments for an intergovernmental approach.

Several developments culminating in 2012 and 2013 caused the United States to reevaluate its relationship with the IANA functions. In 2012, the United States refused to sign a treaty in part out of concern that doing so would lead to increased government control of the internet through a UN body. This led signatories to accuse the United States of hypocrisy; they argued that the United States had an unfair advantage in internet decision-making. Moreover, in 2013, Edward Snowden's disclosures of U.S. intelligence programs led countries to argue that the United States was leveraging its privileged position as a hub of internet traffic for intelligence purposes.

Following these events, the number of calls to alter U.S. government involvement in the IANA functions grew. In March 2014, NTIA announced its intent to transition its oversight of the IANA functions. NTIA asked ICANN to convene internet stakeholders to develop a transition proposal that, among other things, does not replace the U.S. role with a government-led solution. Supporters of the multistakeholder approach immediately welcomed the announcement. Domestic opponents of the transition expressed concern that relinquishing U.S. stewardship would create an opportunity for authoritarian governments to seize control; they argued that, in the absence of direct U.S. control, these governments would work to bring internet governance directly within the ambit of the United Nations. Legislation and litigation exacerbated the appearance that the United States would not relinquish

its privileged position. After two years of consultations, the ICANN-convened group produced a transition proposal that met NTIA criteria. In October 2016, the NTIA contract for the IANA functions expired, beginning a new era in internet governance without direct U.S. stewardship.

CHALLENGES FOR MULTISTAKEHOLDER GOVERNANCE

The reformed multistakeholder internet governance approach faces significant challenges. The sophistication of cybercrime continues to increase, as does the use of computer attacks for espionage, disruption, and influence by states. In October 2016, unknown actors used thousands of unsecured devices to launch a massive attack that limited many users' access to Twitter, Amazon, and other major websites. Left unchecked, these growing threats and other technical vulnerabilities could cripple the internet. Developing economies are only now beginning to grapple with these challenges as increasing numbers of their citizens go online. If the multistakeholder model is seen as ineffective in addressing the vulnerabilities that enable cybercrime, or being completely peripheral to the issue, developing economies could question its legitimacy and seek answers in the multilateral system.

In addition, authoritarian governments, many of which are increasing their efforts to control internet activity within their own borders, continue to challenge multistakeholder models of governance. These countries cherry-pick multilateral and other standards organizations to find those most likely to promote a state-centric approach to governance. Recent efforts to create a technical standard to catalogue all devices connected to the internet failed, but it can be expected that China, Russia, and others will find new opportunities to promote other standards that could frustrate innovation.

There are also worries that ICANN, the operator of the IANA functions, will abuse its authority and ignore the interests of internet users. In the past, ICANN has been accused of ignoring the views of governments, prioritizing private sector interests, and mismanaging its finances. ICANN recently implemented enhancements to address these and similar concerns. Nevertheless, ensuring that ICANN remains accountable will be critical to demonstrating that the multistakeholder approach works. It will also act as a bulwark against Russian and Chinese efforts at greater intergovernmental control over the internet.

RECOMMENDATIONS

Given President Trump's campaign statements, the U.S. government might attempt to reverse the IANA transition, possibly through lawsuits or by unilaterally reimposing NTIA's oversight function. Such a move would be a grave mistake. It would signal that Washington is not committed to the multistakeholder model and would validate Russian and Chinese arguments that the United States seeks to control the internet. It would also incense emerging economies such as Brazil and India that have traditionally advocated for more multilateral control but have softened, or in some cases reversed, their positions as a result of a combination of intense U.S. lobbying and domestic pressure.

Reversal of the transition would also undermine ICANN's critical operations beyond administering the IANA functions, such as managing domain names. The appearance that ICANN is susceptible to the whims of the U.S. government threatens the integrity of its decision-making processes, which may discourage businesses and civil society groups from continuing to voluntarily participate in them. ICANN works because these groups contribute to ICANN decisions that affect their business operations and interests. If the Trump administration reverses course, it would signal to these groups that their decision-making authority is limited and sap their incentive to participate, effectively gutting the multistakeholder model.

Short of reversal, the Trump administration might choose to distance itself from internet governance matters to delegitimize a model it does not believe in. This too would be a mistake because it would reduce U.S. influence over internet policy and leave authoritarian regimes to fill the vacuum.

The viability of the reformed governance approach rests in responsible collective action by all stakeholders. Ongoing instability and rising cyber threats can indirectly support arguments for government control of the internet. To counter these arguments, the United States needs to prioritize two sets of policies that will reduce critical internet vulnerabilities, build trust, and empower newcomers to the internet governance process.

First, the U.S. government should lead by example and launch an effort to improve network stability and security. For years, internet engineers have flagged known vulnerabilities in routing protocols and other critical internet functions that have not received adequate attention, partly because businesses often cut corners on security concerns in order to be first to market. As more devices connect to the internet, this challenge will only grow. Drawing on the work of existing standards bodies and other governments, the United States should foster a multistakeholder process led by the Department of Commerce to identify the most pressing vulnerabilities that need to be remedied. President Trump, given his repeated emphasis on the need to improve cybersecurity, should work with the private sector to launch a global effort to develop and implement solutions to these challenges. The effort could be modeled on the U.S. Global Connect Initiative, which seeks to expand internet connectivity in partnership with the private sector, international development banks, and nonprofits. A cybersecurity-focused initiative would improve the internet's reliability, elevate the multistakeholder model in security discussions, demonstrate that—contrary to the arguments of authoritarian regimes—discussion on internet security is incomplete when involving only states, and maintain U.S. leadership.

Second, the United States should expand its collaboration with industry to increase the technical and policy capacity of government officials, business people, tech experts, and civil society activists abroad, particularly in larger markets such as Brazil, Indonesia, India, Nigeria, and South Africa. The United States has a history of training individuals to increase their likelihood of supporting U.S.-aligned policy solutions. In 1982, U.S. diplomats worked with private companies to form the United States Telecommunications Training Institute (USTTI). It offers tuition-free technology courses to communications professionals, regulators, and entrepreneurs from the developing world. More of these developing-world professionals should be trained if the United States hopes to maintain its influence. This would complement the work of ICANN and other nonprofits that offer similar fellowships.

These fellowship and training opportunities also help the United States in the battle to affect policy through technical standards. As developing countries improve their technical and policy capacities through U.S. and like-minded assistance, they will be better prepared to understand the limitations and economic implications of restrictive policies proposed by authoritarian governments.

Over the decades of the internet's development, multistakeholder governance has adapted to the needs of those who help run the internet and ensure it flourishes. Expanding participation in this process by educating newcomers to its intricacies supports its endurance and equips participants with the tools to work within the model rather than cripple it. Most important, having more private sector and civil society participation in internet governance actually makes the United States more influential. Despite their differences post-Snowden, the interests of private sector and Western civil society actors are much more likely to be aligned with the United States than with Russia or China, making intergovernmental control of the internet less likely.

Following the IANA transition, the internet remains a resilient platform. Yet it continues to face technical and policy challenges that may limit its long-term utility. Without sustained leadership, authoritarian governments will capitalize on these challenges that could limit global economic growth and result in severe content control. To prevent this, the U.S. government should promote the development of technical solutions to enhance the internet's reliability and resilience, and participate in initiatives involving all stakeholders to bring the next billion users online. It is in the United States' strategic interest for internet governance to remain a priority.

About the Author

Megan Stifel is an attorney and the founder of Silicon Harbor Consultants, a firm that provides strategic cybersecurity operations and policy counsel. She is also a nonresident senior fellow in the Atlantic Council's Cyber Statecraft Initiative. She previously served as a director for international cyber policy at the National Security Council (NSC), where she was responsible for expanding the Barack Obama administration's cybersecurity policy abroad, including in connection with internet governance, bilateral and multilateral engagement, and capacity-building. Prior to her time at the NSC, Stifel served in the U.S. Department of Justice (DOJ) as director for cyber policy in the national security division, and prior to that, as counsel in the DOJ's computer crime and intellectual property section. A frequent lecturer on cybersecurity, she has been quoted in numerous publications, most recently *SC Magazine* and *Politico Pro*. Prior to law school, Stifel worked for the U.S. House of Representatives Permanent Select Committee on Intelligence. She received a BA in international studies and German from the University of Notre Dame and a JD from Indiana University's Maurer School of Law.

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 aims to identify solutions to one of the world's most pressing challenges in the twenty-first century: keeping the global Internet open and secure in the face of unprecedented threats. Through briefings, reports, and the *Net Politics* blog, the program produces research and analysis on the politics of cyberspace. Cyber Briefs are short memos that provide concrete recommendations on topics related to online privacy, cybersecurity, Internet governance, 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.