BROWN

Savage, John <john_savage@brown.edu>

China, EU seize control of the world's cyber agenda - POLITICO

John Savage <john_savage@brown.edu> Tue, Jul 24, 2018 at 11:12 AM
To: John Savage <John_Savage@brown.edu>

https://www.politico.com/story/2018/07/22/china-europeglobal-cyber-agenda-us-internet-735083

China, EU seize control of the world's cyber agenda

The U.S. guided global internet policy for decades. Now, the EU and China are taking the lead.

ERIC GELLER 07/22/2018 07:01 AM EDT

European Commission President Jean-Claude Juncker, left, greets China's Foreign Minister Wang Yi prior to a meeting at EU headquarters on June 1. Beijing and Brussels are effectively writing the rules that may determine the future of the internet. | Virginia Mayo/AP Photo

The United States is losing ground as the internet's standard-bearer in the face of aggressive European privacy standards and China's draconian vision for a tightly controlled Web.

The weakening American position comes as the European Union, filling a gap left by years of lax U.S. regulations, imposes data privacy requirements that companies like Facebook and Google must follow. At the same time, China is dictating companies' security practices with mandates that experts say will undermine global cybersecurity — without any significant pushback from the United States.

Story Continued Below

The result: Beijing and Brussels are effectively writing the rules that may determine the future of the internet. And China's vision is spreading across the developing world as it influences similar laws in Vietnam, Tanzania and Nigeria.

Experts in cyber policy say the trends could slow the internet's growth, stunt innovation and erect new market barriers for American businesses. And while these trends began before Donald Trump became president, his administration has yet to devise a clear plan to rebut either of these agendas.

"The U.S. cannot afford to be on the sidelines," said Chris Painter, America's top cyber diplomat from 2011 to 2017, who is now with the Global Commission on the Stability of Cyberspace. "Other countries are doing things legislatively that affect the U.S. … and the U.S. is on the back foot."

One result of this shift is the erosion of the freewheeling U.S. vision of the internet that had reigned for decades. "The U.S. model looks both paralyzed and somewhat feckless, while the Europeans and the Chinese are making progress and, in many cases, damaging the openness of the internet," said Adam Segal, director of the Council on Foreign Relations' cyber policy program. "And we don't particularly have a coherent response to it."

The lack of U.S. leadership also harms ordinary Americans by letting industry block the adoption of strong protections against cyberattacks, said Sen. Ron Wyden (D-Ore.), one of Congress' leading voices on cybersecurity and technology issues.

"The United States is failing on cybersecurity because our Congress has been captured by corporations who have successfully killed any effort to impose meaningful cyber standards," he told POLITICO in an email.

For years, the U.S. objected aggressively when China and other authoritarian regimes tried to co-opt international venues to push their cyber agendas. In 2015, China, Russia, Kazakhstan, Kyrgyzstan, Tajikistan and Uzbekistan introduced a "code of conduct for information security," which would have codified their vision of content regulation, but behind-the-scenes work by Western governments halted its momentum. The U.S. blocked similar efforts at a United Nations technology commission. And in 2010, the U.S. helped prevent a vote to hand a role in internet policymaking to the International Telecommunications Union, which would have given a stronger hand to authoritarian countries that often lose to the West in other settings.

Story Continued Below

"In all bilateral and multilateral encounters heretofore, the United States has successfully and consistently, in a bipartisan way, opposed" authoritarian visions for cyberspace, said a former State and Commerce department official who spent eight years working on cyber issues and requested anonymity to speak candidly.

But the U.S. has offered only token opposition to the cybersecurity law that China imposed last year, which among other things requires companies operating in China to provide authorities with the source code to their software.

The U.S. has taken a much more modest approach to its own cybersecurity policy: It passed a cyber information sharing law in 2015 that gave companies legal immunity for sharing threat data with the government, and the National Institute of Standards and Technology introduced a voluntary "framework" for managing digital security risks. Industry groups praised these efforts, saying they influence policies worldwide.

But beyond these piecemeal steps, the U.S. has advanced no coherent vision of cybersecurity regulation to counter the ones from China and Europe. And Russia will soon try again with its cybersecurity "code of conduct" — with vague language discouraging interference in other states' internal affairs — at the U.N. General Assembly in September.

The U.S. is at a disadvantage, Painter said, because while China and others roll out ambitious plans, American diplomats call for only modest reforms. "If the U.S. line is, 'Leave the status quo as it is,' that's always hard," he said.

Chinese Communist Party leaders see cybersecurity "as a fundamental part of their governance model," said Samm Sacks, a senior fellow at the Center for Strategic and International Studies. And President Xi Jinping has taken a personal interest in the topic, beyond how most world leaders engage with the issue.

Meanwhile, Beijing's grip on domestic affairs gives it an advantage over the U.S. when it comes to laying down the law.

Story Continued Below

The result is China's cybersecurity law, which took effect on June 1, 2017, creating vaguely defined inspection regimes for network operators and critical infrastructure owners. These businesses must let Chinese officials test their equipment and software at any time. They must also store their data in China so investigators can access it. One provision could let Beijing demand companies' decryption keys, which would effectively ban the unbreakable encryption found in apps like Signal.

But even as the fractious Chinese bureaucracy prepared to implement the law, Beijing was busy promoting its view of digital security controls abroad, focusing on developing nations that it hopes will join a coalition to counter the West's more open internet agenda.

In a digital extension of its sweeping One Belt One Road initiative, China spent vast sums to expand internet connectivity in small and underdeveloped countries. It donated computers to governments in nearly three dozen countries, from Pakistan to Malawi to the small island state of Tonga. Huawei, the Chinese telecom giant that U.S. officials consider a cybersecurity risk, set up armies of security cameras in the Kenyan cities of Nairobi and Mombasa as part of its "Safe City" initiative.

Cyber experts suspect China's generosity is driven by its strategic self-interest: Beijing wanted to have a foothold in these emerging countries' computer networks. Evidence has occasionally emerged to support this view. In January, the French newspaper Le Monde reported that China had spent years spying on the African Union, whose headquarters it built and donated to the international organization in 2012. Buried in the facility's ready-made computer network, the paper said, were backdoors letting Beijing monitor the African Union's activities.

"China's influence is second to none in terms of its relationships with developing countries and in terms of its expanding relationship, recently, with developed countries," said the former State Department official. As a result, he said, "Chinese companies are essentially the lead [and] have inside access" to countries' systems.

The U.S. government and American corporations also must deal with a newly aggressive Europe on cyber issues. In August 2016, the EU enacted its first major cyber law, which requires "operators of essential services" to "take appropriate and proportionate … measures to manage" their cyber risks. The EU is now considering another law that would task its cyber agency, ENISA, with certifying security products in EU member states.

Both of these laws will force U.S. companies with European footprints to redesign their security measures to comply, and the more they do so, experts said, the more the EU position becomes the default. The same is true for the EU's General Data Protection Regulation, which imposes tough data privacy and disclosure requirements — including the threat of massive fines for companies that violate them — and could undermine cybersecurity.

Story Continued Below

The White House is discussing introducing a GDPR competitor, according to news reports, but it may be too late — the European rule effectively kneecapped the United States' ability to set global privacy standards at a lower level. "If you're a company," said the former State Department official, "you have to abide by the stricter standard."

The question for the U.S. is whether to abandon its insistence on a voluntary, industry-led approach and enact more regulations that reflect a clear U.S. vision. Many experts said the American tradition of letting the private sector shape the debate has undercut the nation's standing globally.

Other countries "have looked around and said, 'All right, this doesn't really seem to be accomplishing very much,'" Segal said.

One option would be to follow China and the EU in passing a sweeping national cyber law. If it took a light touch but still imposed rules, and if the U.S. could demonstrate that it improved security, other countries would take note. But as recent history shows, such a law would have a difficult chance of passing Congress.

James Lewis, a cyber expert at CSIS, said the U.S. is the only country where extreme distrust of government prevents meaningful cyber regulations. "That's not how it works in the rest of the world," he said. "And I say that for both democracies and dictatorships. This overwhelming angst we have about government is not reflected anywhere else on the planet."

Industry executives say regulations aren't the answer. Chris Boyer, assistant vice president of public policy at AT&T, said the best "opportunity for the U.S. to proactively lead this conversation" lies in voluntary standards.

But many security experts argue that isn't enough. "These voluntary frameworks," said Segal, "have not really, as far as we can tell, improved U.S. security significantly."

Regardless of how the U.S. moves forward, experts said it must engage more aggressively in the international debate. "We should try to provide a clear road map of the type of approach we want to see other countries adopting," said the former State official. "Silence just cedes the ground to other views and other approaches that we fundamentally disagree with."

Story Continued Below

Sustained engagement will require a strategy on the part of the Trump administration. For now, the former official said, U.S. diplomats attending these meetings "don't say anything" and are "not relevant."

The administration's cyber leadership void has exacerbated the problem. National security adviser John Bolton eliminated the White House cyber coordinator role, the central figure overseeing all U.S. cyber activities, and former Secretary of State Rex Tillerson nixed Painter's top cyber diplomat role. A deputy assistant secretary of state, Rob Strayer, now manages cyber diplomacy, though a bill to elevate his office is nearing passage.

The State Department did not make Strayer available for an interview about the U.S. strategy.

"The degradation or the removal of certain roles is hugely important," said Josh Kallmer, senior vice president for global policy at the Information Technology Industry Council. He said his meetings with administration officials often involve "trying to reverse those things."

The battle isn't over yet, and China's agenda still faces hurdles. For one thing, although its cyber law is technically in place, many of its provisions have not yet been enacted, and regulatory agencies are competing over how to implement it. Plus, Chinese firms that want to dominate global markets are pushing back on Beijing's attempt to balkanize the internet.

"There are constraints internally in China's system that are going to be a check on some of the more alarming parts of this vision," Sacks said.

But even so, China is making a greater effort than the U.S., and the EU isn't far behind. "For the first time," said the former State Department official, "many, many, many countries … rank much higher in influence than the U.S."

Lewis, reflecting on his recent conversations in Europe and Asia, was pessimistic. "The internet is going to be regulated, and it'll be regulated from Brussels and Beijing," he said. "We're kind of out of it, because we don't have a good counter."

Missing out on the latest scoops? Sign up for POLITICO Playbook and get the latest news, every morning — in your inbox.

Show Comments

Sent from my iPhone