

LOUISE MATSAKIS SECURITY 11.12.18 07:37 PM

THE US SITS OUT AN INTERNATIONAL CYBERSECURITY AGREEMENT



BERTRAND GUAY/AFP/GETTY IMAGES

DURING A SPEECH at the annual UNESCO [Internet Governance Forum](#) in Paris Monday, French President Emmanuel Macron announced the “[Paris Call for Trust and Security in Cyberspace](#),” a new initiative designed to establish international norms for the internet, including good digital hygiene and the coordinated disclosure of technical vulnerabilities. The document outlines nine goals, like helping to ensure foreign actors don’t interfere with elections and working to prevent private companies from “[hacking back](#),” or retaliating for a cybercrime. It’s endorsed by more than 50 nations, 90 nonprofits and universities, and 130 private corporations and groups. The United States is not one of them.

The Paris Call ultimately lacks teeth; it doesn’t require governments or corporations legally adhere to any specific principles. It’s mostly a symbol of the need for diplomacy and cooperation in cyberspace, where it’s hard to

Facebook, Google, IBM, and HP all endorsed the agreement.

The United States, meanwhile, was not alone in taking a pass. Russia, China, Iran, and Israel didn't sign, either.¹ Some of the abstainers, like China and Iran, have active cyberwar initiatives.

Microsoft, on the other hand, says it worked closely with the French government to craft the Paris Call, a sign of how tech corporations are playing a more active role in governing the internet.

“It’s an opportunity for people to come together around a few of the key principles: around protecting innocent civilians, around protecting elections, around protecting the availability of the internet itself. It’s an opportunity to advance that through a multi-stakeholder process,” says Brad Smith, the president of Microsoft, who also gave a speech in Paris Monday. In some ways, Smith sounds more like a lawmaker than an executive—which shouldn’t come as much of a surprise.

On the internet, corporations like Microsoft are increasingly taking on responsibilities once reserved for nation states. “If you look over the past three or four years, we’ve really seen a groundswell of private leadership,” says Megan Stifel, the cybersecurity policy director at Public Knowledge, a non-profit that endorsed the Paris Call. “The private sector is now willing to say that we can and we will do more.”

In April, Microsoft announced the [Cybersecurity Tech Accord](#), an agreement similar to the Paris Call that was signed by more than 60 technology corporations, which it dubbed a “a Digital Geneva Convention.” In July, the company publicly advocated for the regulation of facial recognition technology and said it was developing its own set of principles for how it should be used. Then in August, Microsoft took action against the hacking group known as Fancy Bear. In an announcement that could have just as plausibly come from the FBI, the company went so far as to attribute the series of malicious domains it seized as having originated from Russia.

It’s not just Microsoft: In August, Facebook and Twitter worked with US government authorities to take down accounts and pages they believed were

elections, in an effort to ensure the voting process wasn't being disrupted.

Combating cyberattacks and monitoring elections were once tasks reserved for government officials. But now much of the globe's civic activity occurs not just in cyberspace, but on private platforms owned by companies like Facebook and Microsoft. That means it's in their business interest to support measures like the Paris Call, which aim to make the internet a more secure and predictable place.

Not every group that supports the Paris Call agrees with all of its tenets. Access Now, an international non-profit that advocates for a free and open internet, criticized two parts of the agreement in a [blog post](#) published Monday. The agreement calls for stakeholders to cooperate to address the threat of "cyber criminality," but Access Now worries that could be interpreted to mean companies and governments should share data without a court order, for instance. The Paris Call also advocates for the prevention of intellectual property theft, but the nonprofit thinks that could end up putting freedom of expression at risk if states are overly aggressive.

"The document is imperfect but it arrives as other governments, that did not endorse the Paris Call, have shown a competing vision for cybersecurity grounded instead in state sovereignty and control," says Drew Mitnick, policy counsel at Access Now. Mitnick says his organization is looking forward to the next iteration of the Paris Call, which is set to reconvene next year in Germany.

In the meantime, the agreement's organizers will likely continue to try to get nations like the US on board, while the country's largest tech companies keep leading the way.

¹ **CORRECTION 11/13/18 9:30 AM:** *A previous version of this article incorrectly included the United Kingdom among the countries that did not sign the Paris Call for Trust and Security in Cyberspace. The UK is a signatory, and we have updated the story accordingly.*

- Learn to fly Sikorsky's new helicopter in just 45 minutes
- iPads are officially more interesting than MacBooks
- How does gaming affect your body? We tried to find out
- The AI cold war that threatens us all
- Looking for more? Sign up for our daily newsletter and never miss our latest and greatest stories

RELATED VIDEO

WATCH



How to Protect Yourself After a Massive Corporate Hack

SECURITY

How to Protect Yourself After a Massive Corporate Hack

It seems like every time you turn around there's a new breach of personal information. Follow these steps to minimize the damage.

#CYBERSECURITY #FRANCE #MICROSOFT #POLICY

MORE SECURITY

SECURITY ROUNDUP

Taylor Swift's Facial Recognition Scans Crowds for Stalkers

BRIAN BARRETT

0000

SOCIAL MEDIA

At a New York Privacy Pop-Up, Facebook Sells Itself

LOUISE MATSAKIS

HOAXES

Nationwide Bomb Threats Are a New Spin on an Old Bitcoin Scam

EMILY DREYFUSS

HACKING

Facebook, Under Scrutiny, Pays Out Largest Bug Bounty Yet

LILY HAY NEWMAN



RUSSIA PROBE

9 Trumpworld Figures Who Should Fear Mueller the Most

GARRETT M. GRAFF

GET OUR NEWSLETTER

Enter your email

SUBMIT

FOLLOW US ON YOUTUBE

Don't miss out on WIRED's latest videos.

FOLLOW

SUBSCRIBE

ADVERTISE

SITE MAP

PRESS CENTER

FAQ

ACCESSIBILITY HELP

NEWSLETTER	WIRED STAFF
JOBS	RSS

CNMN Collection

© 2018 Condé Nast. All rights reserved.

Use of and/or registration on any portion of this site constitutes acceptance of our [User Agreement](#) (updated 5/25/18) and [Privacy Policy and Cookie Statement](#) (updated 5/25/18). [Your California Privacy Rights](#). The material on this site may not be reproduced, distributed, transmitted, cached or otherwise used, except with the prior written permission of Condé Nast. [Ad Choices](#).
