New York Times (Nov. 13, 2018)

U.S. Declines to Sign Declaration Discouraging Use of Cyberattacks

WASHINGTON — Reflecting reluctance by the Trump administration to limit its options for using offensive and defensive cyberweapons, the United States declined on Monday to sign a vaguely worded international call to protect civilians against cyberattacks and discourage digital meddling in elections.

The United States was one of only a few Western nations that chose not to sign on to the nonbinding declaration, which was released by France's president, Emmanuel Macron, during the Paris Peace Forum, timed to the 100th anniversary of the end of World War I.

The declaration, the "Paris Call for Trust and Security in Cyberspace," was signed by 51 countries, more than 130 companies and 90 universities and nongovernmental groups, and was the latest in a series of efforts to move toward what some call a "digital Geneva Convention."

Just as the original Geneva Convention prohibits aiming attacks at civilians, the Paris statement would prohibit "indiscriminate or systemic harm to individuals and critical infrastructure," such as shutting down an electric grid.

It also included a call to "prevent malign interference by foreign actors aimed at undermining electoral processes though malicious cyberactivities."

All members of the European Union signed the agreement. Australia and Turkey joined the United States in declining.

Mr. Macron aimed the accord largely at democracies, which meant that the countries most often accused of conducting state-sponsored attacks — Russia, China, North Korea and Iran — did not participate in the process.

Israel, which along with the United States conducted the most sophisticated cyberattack in history, the Stuxnet attack on Iran's nuclear enrichment program, also declined to sign.

The United States did not say why it did not sign the accord, and one diplomat, who would not allow the use of his name because he is not authorized to speak publicly on policy issues, said that it was possible that Washington may sign the principles at a later date.

But if past debates over setting norms of behavior for cyberspace are a guide, American officials are leery of any kind of agreement that might make illegal the types of activity — like espionage, data manipulation or attacks on infrastructure — that the United States may want to use in a future conflict.

Elections are an interesting example. Congress and many others have condemned the 2016 Russian attacks on the Democratic National Committee and the private email accounts of senior officials in Hillary Clinton's presidential campaign. But the United States has interfered in foreign elections before, including Italy in the 1940s and Iran and Latin America in the 1950s and 1960s, and some officials say that no American president should be forced to give up that tool if it could prevent a war.

Similarly, the Pentagon worries about commitments to avoid using cyberattacks as a prelude to military action. The United States had a secret program, code-named "Nitro Zeus," which called for turning off the power grid in much of Iran if the two countries had found themselves in a conflict over Iran's nuclear program. Such a use of cyberweapons is now a key element in war planning by all of the major world powers.

Still, the fact that companies and governments came together on any kind of vision for keeping the internet free of malicious activity was viewed by some key players as a step forward.

"Most of the world's democracies are rallying around the need to protect all democracies from cyberattacks," said Brad Smith, the president of Microsoft, who has been among the most vocal in arguing for a digital Geneva Convention. "You have to start by building a strong coalition among the democracies themselves."

Much of the statement of principles calls for restrictions on actions Washington has also condemned in the past: the theft of intellectual property, including trade secrets and industrial designs, and attacks on "the public core of the internet."

The United States has indicted Chinese, North Korean, Iranian and Russian hackers for offenses including theft of industrial secrets and for attacking Sony Pictures

Entertainment to prevent the distribution of a movie that North Korea found offensive. Nonetheless, the administration's aversion to international agreements in general may have made it leery of joining the announcement on Monday.

Governments were outnumbered by companies and nongovernmental groups as signatories. Google, Facebook, Microsoft and I.B.M. all signed on. Three of the five countries that are part of what is known as the "Five Eyes," — the English-speaking victors of World War II who share intelligence information — also signed: Britain, Canada and New Zealand.