The suspected Russian hack of U.S. government agencies has led to heated rhetoric from lawmakers, with U.S. Senator Dick Durbin calling it “virtually a declaration of war” and U.S. Senator Marco Rubio saying that “America must retaliate, and not just with sanctions.”

But cybersecurity and legal experts said the hack would not be considered an act of war under international law and will likely go down in history as an act of espionage.

Here’s why.

What do we know about the Hack?

The hack, first reported by Reuters, hijacked software made by Texas-based SolarWinds Corp. By inserting malicious code into updates pushed to SolarWinds customers, the hackers were for months able to explore the computer networks of private companies, think tanks, and government agencies.

Sources familiar with the U.S. investigation said the hack was likely carried out by Russia’s foreign intelligence service. Moscow has denied involvement.

The magnitude of the hack is still unclear, but hackers are known to have monitored email or other data within several U.S. government agencies.

The breached federal agencies include the Commerce Department, Treasury Department, and Department of Energy.

An Energy Department spokeswoman said malware had been “isolated to business networks only” and had not impacted U.S. national security.

Was the hack an ‘Act of War’?

It is too early to say for sure, but probably not, according to cybersecurity experts.

To qualify as an act of war, United Nations resolutions and other sources of international law require a certain level of force or destruction that does not appear to be the case this

time.

“Warfare implies violence, death and destruction,” said Duncan Hollis, a professor of law at Temple University specializing in cybersecurity.

Hollis and other experts said the attack appears to have been carried out to steal sensitive U.S. information, and should be viewed as espionage.

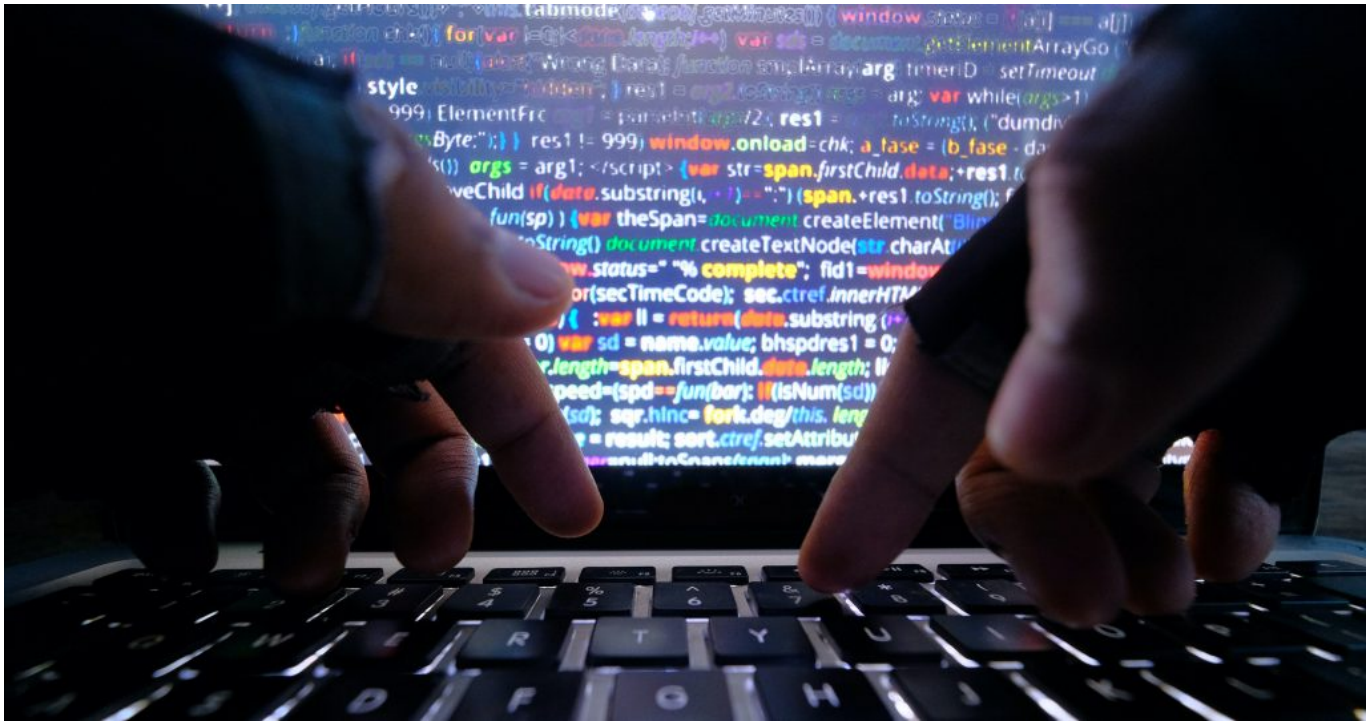
“Simply stealing information, as much as we don’t like it, is not an act of war — it is espionage,” said Benjamin Friedman, a policy director at the think tank Defense Priorities.

Experts said cyber attacks can be acts of war if they cause physical destruction.

A Department of Defense law of war manual states that some cyber operations should be subject to the same rules as physical, or “kinetic” attacks. Examples include operations that “trigger a nuclear plant meltdown; open a dam above a populated area, causing destruction; or disable air traffic control services, resulting in airplane crashes.”

John Bellinger, the top State Department lawyer under former Republican Secretary of State Condoleezza Rice, said it was not yet clear whether the hack could be considered an act of war.

“It may simply be a massive act of espionage that would not constitute an act of war. We don’t know yet whether the Russians simply accessed U.S. government computers or actually disrupted government functions,” said Bellinger, a senior fellow at the Council on Foreign Relations think tank.



Is there any precedent for the hack?

A hack in 2014 that targeted the U.S. government's personnel agency, the Office of Personnel Management, exposed sensitive personal information of millions of current and former federal employees and contractors.

Former Director of National Intelligence James Clapper said in 2015 that he suspected China of conducting the hack, and he said during congressional testimony two years later that in his view it was an act of espionage.

"I think there is a difference between an act of espionage, which we conduct as well, and other nations do, versus an attack," Clapper said at the time.

A devastating 2017 hack attributed to Russia, known as "NotPetya," crippled ports by paralyzing the shipping giant A.P. Moller-Maersk and other global corporations.

Olga Oliker, a Washington-based expert on U.S.-Russia relations, said in 2017 testimony before the U.S. Senate that, if Russia was to blame for NotPetya, "it is an example of precisely the type of cyber operation that could be seen as warfare, in that it approximates effects similar to those that might be attained through the use of armed force."

How might the United States respond?

The Defense Department manual says the United States cannot use force to respond to a cyber operation that is not itself an act of force. Instead, the United States can respond with measures such as “a diplomatic protest, an economic embargo, or other acts of retorsion” the manual says.

“We know that lots of countries engage in espionage, and we don’t bomb them in response,” said Friedman.

U.S. President-elect Joe Biden signaled on Thursday that he would use targeted financial sanctions to respond.

“They’ll be held accountable,” Biden told The Late Show with Stephen Colbert. “Individuals, as well as entities, will find … there are financial repercussions for what they did.”

The views and opinions expressed in this article are those of the author and do not necessarily reflect the views of The Kootneeti Team