US needs top cyber coordinator, better hacker 'deterrence': panel

March 11 2020

A congressional commission made more than 80 recommendations to improve US cyber defenses including the appointment of a caninet-level cybersecurity coordinator

The US needs a top-level cybersecurity coordinator and a better strategy of "deterrence" to protect against hackers and other cyber threats, a congressionally mandated commission said Wednesday.

Defense in cyberspace requires a series of government reforms and policies to strike back at attackers, according to the report by the Cyberspace Solarium Commission.

The bipartisan panel which included lawmakers and private sector experts made more than 80 recommendations ranging from reforms in the executive and legislative branches to better cooperation with allies to secure cyberspace.

"The reality is that we are dangerously insecure," said a statement from Senator Angus King and Representative Mike Gallagher, co-chairs of the panel which took its name from an Eisenhower-era foreign policy project.

"Your entire life—your paycheck, your health care, your electricity—increasingly relies on networks of digital devices that store, process and analyze data. These networks are vulnerable, if not already compromised."

Panel members described the required effort as equivalent to preventing another 9/11 attack.

The panel recommended the establishment of White House cabinet-level "national cyber director" to direct coordination within government and the private sector.

Additionally, the panel cited the need for a stronger deterrence strategy to demonstrate that attackers in cyberspace would pay a price.

"Deterrence is possible in cyberspace," the report said.

"Today most cyber actors feel undeterred, if not emboldened, to target our personal data and public infrastructure... through our inability or

unwillingness to identify and punish our cyber adversaries, we are signaling that interfering in American elections or stealing billions in US [intellectual property](#) is acceptable."

It said the US government and [private sector](#) must "defend themselves and strike back with speed and agility."

The commission said cyber defense should rely on a "layered" strategy that imposes costs on attackers.

"A key, but not the only, element of cost imposition is the military instrument of power," the report said.

"The United States must maintain the capacity, resilience, and readiness to employ cyber and non-cyber capabilities across the spectrum of engagement from competition to crisis and conflict."

© 2020 AFP