Who is responsible for keeping the cyber domain safe?

Hailey Brown

03/09/2023

Cybersecurity Operations at Port San Antonio

Hailey Brown - Cybersecurity has become a growing geopolitical concern over the last couple of decades, forcing presidential administrations to devise ongoing strategies to quell threats to cybersecurity. The most recent update to the Biden administration's cyber strategy could require companies to develop and adopt broader cybersecurity initiatives and impart consequences if companies' measures prove inadequate. The new strategy also reflects heightened governmental accountability in offensive and defensive cyber processes.

The new responsibilities for corporations are an example of the growing role of non-state actors in the geopolitical arena. State and governmental entities are not the only influential force in geopolitics. Corporations, groups, people, and social movements all share a role in politics. Like traditional actors, they hold geopolitical codes which inform their interactions and relationships on all scales. The Biden administration has used its regulatory power to influence American companies' geopolitical codes, giving them higher requirements for preventing cybercrime and protecting their infrastructure from cyber attacks. While companies have freedom over most processes, there are still government regulations in many industries to uphold standards of safety. In this case, the status quo does and cannot meet the needs of the state, as the threat of cyber attacks has grown alongside the cyber and technological innovation of U.S. adversaries. Thus, the Biden administration is building on the efforts of past presidents to build requirements that will protect American infrastructure and people from cyber threats.

The White House national cyber director, Kemba Walden, called the internet a global commons, meaning it is a universally shared resource, explaining why this new initiative was developed. The cyber domain operates on and impacts many scales, making it important for actors on all levels to be involved in protecting it from outside threats. The federal government cannot maintain security on each scale of the cyber domain by itself, requiring the private sector to take on an expanded role.

Image source: Maj. Christopher Vasquez, USAF, Public domain, via

Wikimedia Commons