US spymaster warns over low-level cyber attacks

February 27 2015

A steady stream of low-level cyber attacks poses the most likely danger to the United States rather than a potential digital "armageddon," US intelligence director James Clapper said on Thursday.

US officials for years have warned of a possible "cyber Pearl Harbor" that could shut down financial networks, poison water supplies or switch off power grids.

But Clapper told lawmakers that American spy agencies were more focused on lower-profile but persistent assaults that could have a damaging effect over time.

"Rather than a 'cyber Armageddon' scenario that debilitates the entire US infrastructure, we envision something different," Clapper told the Senate Armed Services Committee.

"We foresee an ongoing series of low-to-moderate level cyber attacks from a variety of sources over time, which will impose cumulative costs on US economic competitiveness and national security," he said.

The past year had seen "destructive cyber attacks" for the first time on US soil carried out by other countries, Clapper said.

He cited North Korea's alleged hacking of Sony Pictures in November and an Iranian attack a year ago against the Las Vegas Sands Casino Corporation.

Pyongyang was accused of targeting Sony over a comedy film that portrayed the fictional assassination of North Korea's leader. And Iran went after Sands purportedly because the company's CEO, billionaire Sheldon Adelson, is known as a hawkish supporter of Israel.

Foreign "actors" are conducting reconnaissance and gaining digital access to US infrastructure systems, so they can launch a cyber attack if necessary in the future, he said.

Russia and China had particularly sophisticated cyber capabilities, according to the director of national intelligence.

Russia is creating its own cyber command that will be able to orchestrate propaganda and insert malware into adversaries' computer systems, he said.

Countries such as Iran and North Korea have "lesser technical capabilities but possibly more disruptive intent," he said.

Clapper acknowledged America had "offensive capabilities" in cyberspace but offered no details.

But he said there were questions about how to use such weapons and what sort of doctrine would govern digital operations.

"I think the issue, though, is what is the policy? What is it that would achieve cyber deterrence? And that is an issue that, at the policy level, we're still, frankly, wrestling with," he said.

The United States and Israel were reportedly behind an elaborate cyber attack on Iran's nuclear program in 2010 that damaged hundreds of centrifuges. Dubbed "Olympic Games," the operation employed the Stuxnet computer worm that was introduced through an infected USB

flash drive, according to the New York Times.