Cyber threats expanding, new US intelligence assessment says

February 26 2015, byKen Dilanian

(AP)—The U.S. has elevated its appraisal of the cyber threat from Russia, the U.S. intelligence chief said Thursday, as he delivered the annual assessment by intelligence agencies of the top dangers facing the country.

"While I can't go into detail here, the Russian cyber threat is more severe than we had previously assessed," James Clapper, the director of national intelligence, told the Senate Armed Services Committee, as he presented the annual worldwide threats assessment.

As they have in recent years, U.S. intelligence agencies once again listed cyber attacks as the top danger to U.S. national security, ahead of terrorism. Saboteurs, spies and thieves are expanding their computer attacks against a vulnerable American internet infrastructure, chipping away at U.S. wealth and security over time, Clapper said.

If there is good news, he said, it is that a catastrophic destruction of infrastructure appears unlikely.

"Cyber threats to U.S. national and economic security are increasing in frequency, scale, sophistication, and severity of impact," the written assessment says. "Rather than a 'Cyber Armageddon' scenario that debilitates the entire US infrastructure, we envision something different. 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 U.S. economic competitiveness and national security."

Russia, China, Iran and North Korea are the top nation-state cyber threats, the intelligence assessment found. Traditionally, China had been first on that list, but Russia was listed first this year for the first time. Previously, intelligence officials have said that hackers linked to China have been probing the U.S. electrical grid in an effort to lay the groundwork for attack.

Clapper did not elaborate on his cryptic comment about Russia's cyber capabilities, but the written assessment he delivered said that Russia's defense ministry is establishing its own cyber command responsible for offensive activities, "including propaganda operations and inserting malware into enemy command and control systems." The U.S. Cyber Command plans its own offensive operations, about which little is known.

The intelligence assessment noted public reports that detail how "Russian cyber actors" are developing the ability to remotely hack into industrial control systems that run electric power grids, urban mass-transit systems, air-traffic control networks and oil and gas pipelines. "These unspecified Russian actors have successfully compromised the product supply chains of three (control system) vendors so that customers download exploitative malware directly from the vendors' websites along with routine software updates, according to private sector cyber security experts," the assessment said.

The U.S. and Israel are widely cited as having launched a cyber attack on Iran's nuclear program through an industrial control system. The Stuxnet virus reportedly damaged Iranian nuclear centrifuges, proving that a remote computer attack could cause physical destruction.

The assessment noted that U.S. intelligence agencies have improved their ability to figure out who is perpetrating cyber attacks, despite the many ways such attacks can be disguised. Still, the lack of international norms

makes the behavior difficult to deter, the assessment says.

What's more, "the muted response by most victims to cyber attacks has created a permissive environment in which low-level attacks can be used as a coercive tool short of war, with relatively low risk of retaliation."

The assessment said officials are increasingly concerned that cyber attackers will seek to change or destroy crucial data in a way that could undermine financial markets and business confidence.

Beyond cyber, the assessment surveyed an increasingly uncertain world, noting the existence of more terrorist safe havens than at any time in recent history.

"Unpredictable instability is the new normal," Clapper said.

On terrorism, the assessment noted that "Sunni violent extremists" such as the Islamic State group are "gaining momentum" and that the groups "challenge local and regional governance and threaten U.S. allies, partners, and interests."

"The threat to key US allies and partners will probably increase, but the extent of the increase will depend on the level of success that Sunni violent extremists achieve in seizing and holding territory," the assessment says.

Another variable is "the durability of the U.S.-led coalition in Iraq and Syria," the assessment says.

"Homegrown violent extremists continue to pose the most likely threat to the homeland," Clapper said.

Six months into the U.S. campaign against the Islamic State group in

Iraq and Syria, Clapper described a stalemate, with neither side able to "achieve its territorial ambitions."

The growing prominence of Shiite militias in Iraq, and their campaign of "retribution killings and forced displacement of Sunni civilians," threatens to undermine the fight against the Islamic State group, the assessment said.