US Army reviews rules of engagement over cyber threat

June 27 2013

Gen. Martin Dempsey testifies on June 12, 2013 on Capitol Hill in Washington, DC. The US military is reviewing its rules of engagement to deal with the growing threat of cyber crime, Dempsey said Thursday.

The US military is reviewing its rules of engagement to deal with the growing threat of cyber crime, military chief Martin Dempsey said Thursday.

Dempsey, the Chairman of the Joint Chiefs of Staff, the highest-ranking officer in the US military, said the review was in response to soaring cyber attacks.

"The Department of Defense has developed emergency procedures to guide our response to imminent, significant cyber threats," Dempsey said in a speech at the Brookings Institution, a Washington-based think tank.

"We are updating our rules of engagement - the first update for cyber in seven years - and improving command and control for cyber forces."

Dempsey said that since his appointment as head of the Joint Chiefs in 2011 "intrusions into our critical infrastructure have increased 17-fold."

Some 4,000 cyber-security experts would join the ranks over the next four years, while some $23 billion would be spent on tackling the threat.

Dempsey said Cybercom—the US command responsible for combatting cyber-crime—was now organized in three divisions.

One team was in charge of countering enemy attacks, another was tasked with offering regional support while a third was responsible for protecting some 15,000 US military computer networks.

In addition following a presidential directive, the military now had a manual which allowed it to cooperate with the Department of Homeland Security and the FBI in the event of attacks on civilian networks.

Dempsey meanwhile lamented what he described as inadequate safeguards by the private sector.

"Our nation's effort to protect civilian critical infrastructure is lagging," he said. "Too few companies have invested adequately in cyber

security."

In a reference to concerns over the levels of government surveillance on private individuals since the revelations by leaker Edward Snowden, Dempsey said he believed a balance could be struck.

"I understand that the country is debating the proper purpose, and limits, of intelligence collection for national security," he said.

"Let me be clear—these are two different things. One is collecting intelligence to locate foreign terrorists and their domestic co-conspirators; the other is sharing information about malware to protect our critical infrastructure from a different kind of attack."