ASIA PACIFIC, Japan

Date Posted: 26-Mar-2014

Jane's Defence Weekly

Japan establishes cyber defence unit

Kosuke Takahashi
Tokyo
Additional reporting by
Jon Grevatt
Bangkok

The Japanese Ministry of Defence (MoD) on 26 March launched its cyber defence unit (CDU) to handle cyber attacks against the ministry and the Self-Defense Forces (SDF).

The unit, based at MoD headquarters in central Tokyo, comprises about 90 members from Ground, Maritime, and Air SDF.

The unit is under the defence minister's direct control and subject to the guidance and supervision of the SDF C4SC (command, control, communication, and computers systems command), which is in charge of maintenance and operation of the SDF's Defence Information Infrastructure (DII) system and Central Command System.

Members monitor MoD and SDF computer networks around the clock and respond in the event of a cyber attack.

"Safeguarding the information system of the ministry and the SDF is absolutely imperative to protecting Japan's peace and security," Defence Minister Itsunori Onodera said at the unit's inauguration ceremony.

The MoD allocated JPY20.5 billion (USD200.5 million) for cyber-related activities in its fiscal year 2014 budget. This included JPY12.8 billion for the development of the DII and JPY2.4 billion for the development of cyber information-gathering devices, system design, and analysis devices for cyber defence.

COMMENT

Although cyber attacks have increased in severity in recent years, the Japanese MoD has lagged behind its original schedule in establishing the CDU.
The MoD decided to establish a cyber command in 2009 with the aim of establishing it by March 2012.
The requirement was reiterated in Japan's 2011 Defence White Paper and has prompted expanded cyber defence collaboration with the United States, which was forged during an inaugural dialogue in May 2013.
MoD officials said the ministry was forced to review its initial plans because cyber attacks had become more complex and sophisticated. Officials also argue that they have prioritised better infrastructure and manpower than a speed-before-quality organisation that would be unable to cope with mounting threats.
This was disputed by Professor Yoshiyasu Takefuji, a cyber security expert at Keio University in Tokyo. "Unlike the US and the UK, in Japan technical officials who understand cyber security have no power to make a decision," he told *IHS Jane's* on 26 March. "Inexpert civil officials have that power."
Takefuji also argued that the unit will be ineffective unless the MoD recruits external expertise.
It is also unclear to what extent critical national infrastructure - such as major Japanese defence companies - will be protected.
The threat to such infrastructure was highlighted by a cyber attack endured by Mitsubishi Heavy Industries (MHI) in 2011 that infected at least 80 servers and computers.
Reports at the time said the attack hit MHI shipyards at Kobe and Nagasaki, which are building Japan's Souryu-class diesel-electric submarines and Akizuki-class destroyers respectively, as well as its Nagoya Guidance and Propulsion Systems Works factory at Komaki, which license-builds Patriot surface-to-air missile systems.
The Japanese government is also yet to decide whether the CDU should have counterforce capabilities, such as developing and deploying viruses against attackers, as the Constitution only allows the SDF to maintain a defence-oriented policy.