CYBER SECURITY FOR THE DEFENCE INDUSTRY

By Sanjana Sharma, Aerospace & Defense Analyst, MarketsandMarkets

The defence industry has changed dynamically over the past decade. Threats from conventional insurgent activities are no longer the only concerns for the defence industry. Advancement in the field of information technology, up-gradation of existing weapons with intelligence, surveillance, and reconnaissance systems along with increasing volume of classified data gathered systems have necessitated the usage of reliable and enhanced cyber security solutions for the defence industry.

UPCOMING TRENDS

The current cyber security market encompasses a variety of solutions ranging from network security solution to endpoint security, application security, content security, cloud security, and wireless security solutions. These solutions have the capability to perform individual tasks and can be integrated together to from a strong line of defence against sophisticated threats in a multi-layered fashion. Sophistication of cyber-attacks from worms and viruses to enhanced techniques such as zero-day attack, Dynamic Trojan Horse Network (DTHN) Internet worm, and Stealth Bot led the cyber security vendors to design upgraded security software and solutions such as the Integrating Basic Unified Threat Management systems, Security of Information Management (SIM) software solutions, network flow analysis, Next-Generation Firewalls (NGFWs), Security Information and Event Management (SIEM), whitelisting, and DDoS mitigation techniques.

Rising threat of cyber-attacks to critical infrastructures by organised criminal groups along with technological advancement in the cyber security market remains as the key driver for the growth of cyber security solutions for the defence industry. The defence and the homeland security agencies are expected to cover around 40% share of the global cyber security market in 2015. Growth in investments on military programs and allocation of resources for research and development of cyber security solution for the battle field communication systems is expected to remain as the most upcoming trends in the cyber security market for the defence industry over the coming years.

GROWTH REGIONS

Despite of declining defence budget in North America, and the West European region, the global cyber security market for the defence industry is expected to grow significantly over the next decade. Huge investments in cloud network security solutions applicable for the battle field management, data protection, & wireless security solutions along with development of network security & cloud security software stands out as the key factors contributing to the growth of cyber security market for the defence sector.

... THE 2016 FISCAL YEAR BUDGET PROPOSED BY THE U.S. GOVERNMENT HIGHLIGHTED AN OVERALL $14 BILLION FUND ALLOCATION FOR ENHANCEMENT OF CYBER SECURITY SYSTEMS AND PREVENTION OF CYBER-ATTACKS FROM ORGANISED CRIMINAL GANGS ...

The cyber security market in the Middle East region specifically, in Saudi Arabia, UAE, and Qatar is expected to growing significantly over the coming decade. Cyber-attacks on government network portals in Saudi Arabia and UAE over the past three years stirred their governing bodies to invest in development of Unified Threat Management (UTM) cyber security solutions, cyber-attack alarms, and cyber intrusion prevention technology. UAE established the National Electronic Security Authority (NESA) in 2012 with an aim to strengthen its internet network against cyber-attacks. The Saudi Arabian government collaborated with several U.S. based cyber security solutions manufacturers such as Lockheed Martin and IBM to strengthen their internet portals against cyber-attacks. Qatar launched the National ICT Plan in 2015 with an aim to modernise their legal and regulatory framework and enhance their cyber security solutions over the coming years.

Additionally, countries such as the U.S. and U.K. are also expected to witness a robust growth demanding cyber security solutions for the defence sector over the coming few years. Investments in the cyber security operations and growing dependency on the internet network for management of weapon systems remain as the key drivers for the growth of cyber security market in these countries. The 2016 fiscal year budget proposed by the U.S. government highlighted an overall $14 billion fund allocation for enhancement of cyber security systems and prevention of cyber-attacks from organised criminal gangs. The growing vulnerabilities of cyber-attacks on weapon programs led the U.S. government to allocate $160 million to the Energy Department's National Nuclear Security Administration for cyber protection for weapons programs. The U.K. government invested £860 million and launched the National Cyber Security Program for duration of five years in 2011 with an aim to strengthen its internet network and prevent its cyberspace from online crime.

MARKET PLAYERS

The companies catering to the cyber security market can be broadly classified into security vendors, and defence companies. Security vendors consist of

companies engaged in designing, manufacturing, and delivering information security products, services, and solutions to the defence and government organisations. Cisco Systems Inc., IBM Corporation, Intel Security Group, Dell SecureWorks Inc., Symantec Corporation, and Verizon Communications Inc., are some of the most prominent security vendors in the cyber security market. Defence companies engaged in developing cyber security solutions consists of leading players in the defence industry engaged in developing network security solutions and software to prevent cyber-attacks on military software systems. BAE Systems Plc, General Dynamics Corporation, Finmeccanica S.p.A., Lockheed Martin Corporation, Northrop Grumman Corporation, Raytheon Company, and Thales Group are some of the leading defence companies engaged in manufacturing such solutions, globally.

The defence companies and the security vendors possess substantially different strengths and market growth strategies. However, in order to surpass the advanced persistent cyber-attacks by insurgent groups and terrorist organisations the leading manufacturers in the cyber security market adopted strategies such as joint ventures and acquisitions to strengthen their product portfolio and generate long-term profitability. In October 2014, BAE Systems Plc acquired SilverSky, a cloud based security solution provider for $232 million with an aim to enhance its commercial applied intelligence cyber security segment. In April 2015, Raytheon Company entered into a joint venture with Vista Equity Partners and acquire 80% share of Websense, a computer security software provider for $1.9 billion. These acquisitions enabled Raytheon Company to enhance their Intelligence, Information and Services segment and gain a strong foothold in the North American cyber security market.

... WITH INCREASING DEPENDENCY ON INTERNET NETWORK BY THE MILITARY ORGANISATIONS, THE FREQUENCY OF SOPHISTICATED AND ORGANISED CYBER-ATTACKS IS ON THE RISE ...

CONCLUSION

While the defence industry tends to be program focused and slow moving, the cyber security market is technology driven and is growing very rapidly. With increasing dependency on internet network by the military organisations, the frequency of sophisticated and organised cyber-attacks is on the rise. Hence, the major focus of security vendors and defence organisations in the cyber security market should be to design enhanced cloud computing solutions, operating systems, and virtual machine technologies aided with highly reliable and breach free software systems with an aim to defend their cyber space against cyber-attacks from clandestine state and non-state activist groups in the near future. ■

AUTHOR

Sanjana Sharma
Aerospace & Defense Analyst, MarketsandMarkets