CYBERSECURITY: A CALL FOR NATIONAL STRATEGY

By Yajan Dua, Aerospace & Defence Analyst, MarketsandMarkets

In recent years, governments and international organisations have become more focused on cyber security and increasingly aware of the urgency connected with it. Cyber warfare has become the most serious end of the spectrum of security challenges posed by or within the cyberspace. Similar to the tools of conventional warfare, cyber technology can be used to attack the financial institutions, machinery of state, public morale, and the national energy & transportation.

Cyber warfare is viewed as the fifth battle space in conjunction with multi-faceted conflict environment or more traditional arenas of land, sea, air, and space. Threats emanating from cyberspace are disparate, diffuse, and disproportionate in the harm they may cause. The ad-hoc processes put in place for the security of global enterprise today is unable to handle the scale and complexity of managing cyber security risks. Maintaining pace with latest business & technology trends and cyber threats requires an overhaul of the information security process.

Many organisations are coming together to form a cyber-strategy that will guide the development of cyber forces and strengthen their cyber defense and cyber deterrence posture. The focus of the strategy is to build cyber capabilities; to defend network systems and organisations; defend the homeland & national interests against the cyber threats.

Cyber threats pose the gravest national security dangers, which gave birth to Cybersecurity Framework, designed to improve information sharing with the private sector. It highlights the best practices and globally recognised standards to raise the level of cyber security across a country's critical infrastructure and enhance privacy & civil liberties. A country's economic prosperity, national security, and individual liberties depend on the commitment of securing cyberspace and maintaining an open, interoperable, secure, and reliable internet. Cyber-attacks and cybercrimes pose a threat to critical infrastructure in cyberspace and harm the economy by the theft of intellectual property. Cyber threats getting serious and evolving constantly needs to addressed effectively to sustain Internet as an engine for economic growth and a platform for the exchange of ideas.

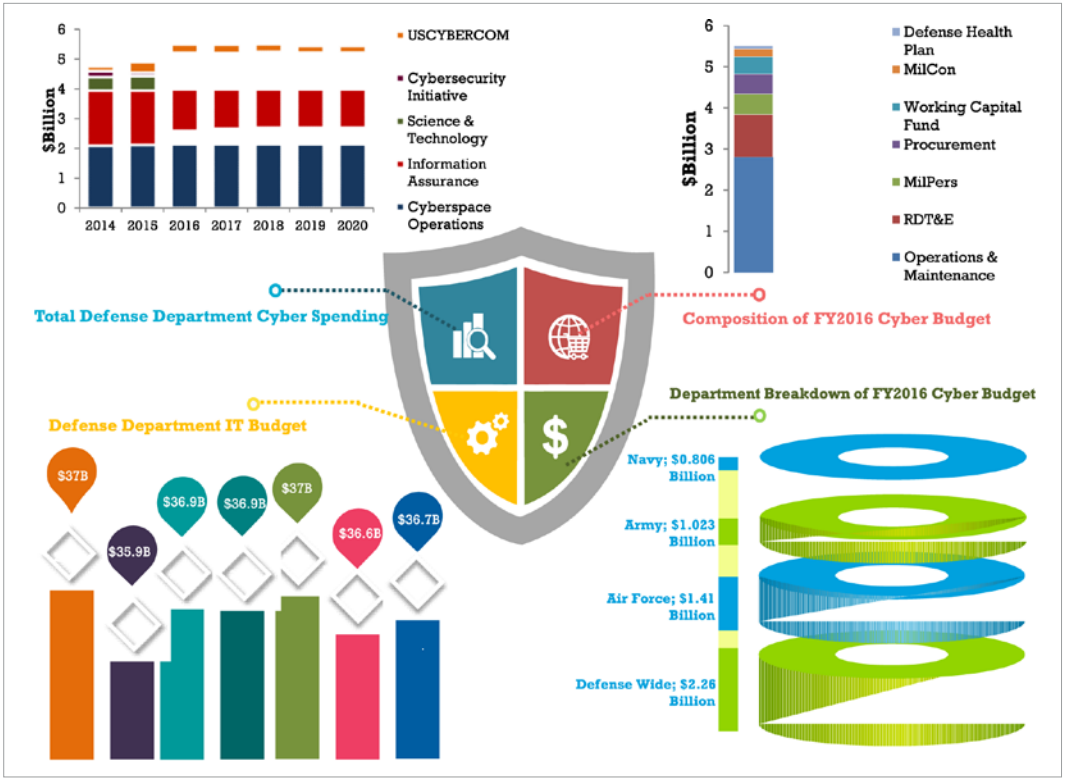
CYBER WARFARE: THE GREAT GAME OF 21ST CENTURY

The global cyber warfare market showcases a productive allure in military and critical infrastructure segment with amplified expenditure on novel technology. Cyber warfare has witnessed dynamic progression from conventional defense approach towards a new-fangled zone. The Cyber security market is projected to show a compelling growth in spending due to ever growing cyber-attack menace in defense and security sectors. Almost every month a major cyber event occurs, encouraging governments to pass new legislation and expand their defense and strategic capabilities.

Considering the magnitude of todays' networks and dilating sophistication of advanced threats, it is almost impossible to reliably safeguard from cyber-attacks and intrusion. In response, organisations' are focusing on more security resources to prevent intrusion towards rapid threat detection and remediation.

The worldwide cyber security market is set to be worth $75.4 billion in 2015 and is expected to register a CAGR of 10.3% and projected to reach more than $155 billion by 2020, as high demand continues for information security solutions. The aerospace, defense, and intelligence vertical continues to be the largest contributor to Cybersecurity solutions.

North America is expected to be the biggest market, while the APAC and EMEA regions are expected to



US Military Cybersecurity by the numbers.

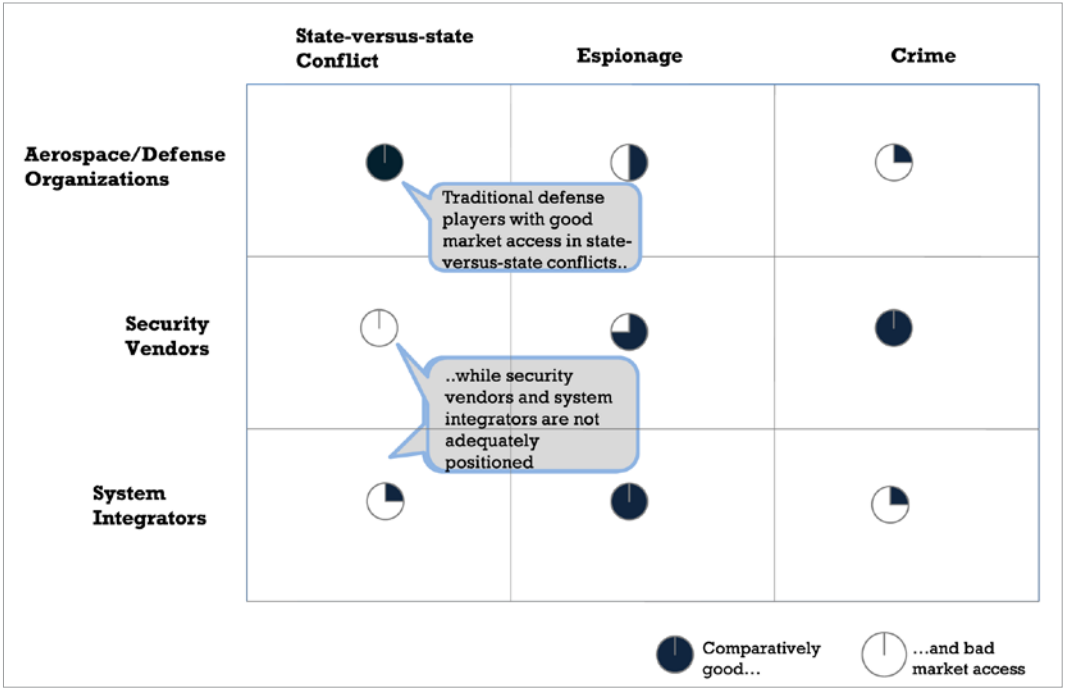
experience increased market traction. Cyber-attacks in South Korea, U.S., Estonia, U.K., and Georgia are anticipated to upswing and spur the market expenditure growth in cyber security configuration, globally.

Countries across regions are now aiming to establish and develop their cyber security infrastructure, an area of defense spending that was neglected until recently. U.S. government estimate worth $50 billion spending on cyber defense from 2010 to 2015, registering a CAGR of 6.2%. The spending doesn't include the commercial investments in developing capability against cyber threats to their enterprises. Moreover, several national governments are strengthening their cyber security organisations to construct defensive and offensive operations. Cyber warfare and cyber espionage are likely to intertwine and slowly subsume conventional warfare.

CYBERSECURITY: A COMPELLING GROWTH FOR DEFENSE COMPANIES

The transformation in the landscape of Cyberspace has led to the evolution in defense sector as a whole new arcade to supplement the present opportunities for defense companies grappling with a shrinking market. The market is dominated by three main groups of players namely, classic security vendors such as Symantec Corporation (U.S.), aerospace and defense companies such as BAE Systems (U.K.), and systems integrators such as AT&T (U.S.).

To succeed in this market, the defense companies and civil players in IT and software development needs to focus on building extensive experience in integrating several parties and handling complex projects. In addition, they need to focus on gaining market share, increase profitability, and providing the right cyber



Positioning & mode of collaboration between defense companies & IT firms.

security solutions. The best practice is to integrate different players and successfully manage joint ventures and collaborations to secure a credible foothold.

The cyber warfare market can be bifurcated on the basis of domination of government and military cyber warfare. Leading companies in cyber warfare market are EADS Group; Airbus Defence & Space (France), BAE Systems (U.K.), Booz Allen Hamilton, Inc., (U.S.), Lockheed Martin Corporation (U.S.), General Dynamics Corporation (U.S.), Raytheon Company (U.S.), and Computer Sciences Corporation (U.S.).

In alignment to the cyber security market estimates, defense companies are assessing growing market opportunities by acquiring civil players with substantially different strengths, either through acquisitions or alliances. When such partnerships are successful, strong growth can be expected, which can ensure long-term profitability.

With information security becoming an ecosystem-wide endeavor, organisations should prioritise a limited number of investments that can deliver the greatest security benefits. An organizations' optimal state of security varies with the changes in its business, risks, and threat environment. Good security is not a one-size-fits-all condition; it's about building capabilities or agility. Security stewardship means continuous assessment and improvement.

ABOUT THE AUTHOR

Yajan Dua, Aerospace & Defence Analyst, MarketsandMarkets