Networked threat: Defence interest in cyber security surges

Date Posted: 30-Mar-2020

Author: **Gerrard Cowan**, Belfast

Publication: Jane's Defence Weekly

Cyber security is a growing priority for armed forces worldwide, boosted by commercial advances in fields like AI and machine learning but held back by a shortage of skilled personnel. Gerrard Cowan reports

Cyber security has captured the attention of the global aerospace and defence (A&D) industry. Companies are pursuing opportunities across various sectors, from hardening satellites to training personnel, while seeking to remain adaptable in the face of continuous change.

This work is driven by the demands of military customers. In a defence context the cyber domain is diverse and yet essential to delivering and protecting capabilities, according to Ed Gillett, sales director of defence and space at BAE Systems Applied Intelligence. The UK-based company is seeing a demand from military customers for securing the data associated with their platforms, both on associated networks and relevant management systems such as those that deal with logistics. To meet this demand companies like BAE Systems must train or hire experts across different fields, Gillett told *Jane's* , including security architecture, federated security, network operations, software engineering, and data science.

There has been a growing focus from customers around understanding the crossover between the cyber and electronic warfare (EW) environments with a view to operating and fighting in those domains, Gillett added. This relies on acquiring the skills of IT professionals, data scientists, and electronic engineers who can deliver an integrated cyber and electromagnetic activities (CEMA) capability.

Personnel from the Marine Corps Forces Cyberspace Command in the cyber operations centre at Fort Meade, Maryland, on 5 February 2020. Cyber security is a growing priority for many armed forces: a situation that has opened up opportunities for the defence industry. (USMC/Staff Sgt Jacob Osborne)

1766967

Diverse portfolios

As interoperability and digital systems play a growing role in defence capabilities, the focus on making these 'secure by design' has sharpened, according to Paul Everitt, chief executive of ADS: the UK trade body representing the aerospace, defence, security, and space sectors. The major area of development is through defence companies diversifying their portfolios, he said.

In the security market the cyber domain is especially prevalent, making up GBP2.1 billion (USD2.5 billion) of the GBP5.2 billion of UK security exports in 2018. This makes it the largest single security capability export, Everitt told *Jane's* , accounting for 40% of sales.

He highlighted a growing focus on supply chain cyber security. In the United Kingdom, for example, some government contracts require accreditation through the Cyber Essentials scheme, which helps to guard against common cyber risks. "This means that high-quality cyber-security services are in demand from industry," he said.

Unlike other areas of military focus, it can be misleading to view cyber security as a standalone area; it is now an essential element of all defence programmes, particularly in the Internet of Things (IoT) era in which many objects and platforms are connected. Defence companies therefore often

adopt an expansive and wide-ranging view of the subject.

For US company General Dynamics Information Technology (GDIT) cyber security is not viewed as a singular part of the company's mission, according to Matthew McFadden, GDIT's cyber director. He described it as "the thread that runs across every endpoint, every network, and every person", adding that it is embedded in all of the company's interests, from its defence business to its internal security operations.

"For our defence programmes, whether it is supply chains, building more resilient systems, or even ensuring the workforce is cyber security qualified and trained, cyber is a central part of their mission and ours from both a customer and company perspective," he told *Jane's* , adding that cyber security is the top priority for chief information officers (CIOs) among the customers of GDIT, which has increased its work with defence and other US government customers over the past five years.

Technological impact

McFadden highlighted various technological trends that are affecting the defence market, including the adoption of 'cloud' or remote computing, containerisation (where software applications run on isolated cloud environments to boost security), and the adoption of 'zero trust architecture', which requires everything to be verified before access is granted.

As such trends develop, McFadden said GDIT is seeing the increased adoption of multi-cloud setups as well as capability development to support monitoring across hybrid capabilities. The increased use of cloud-based containers is the most important element of this work.

Such broad trends are the backdrop to recent plans such as the US Department of Defense (DoD) Cloud and software development, security, and operations (DevSecOps) strategies, the latter being a software engineering culture that aims to unify these three elements. The wide-ranging approach sees security and functional capabilities being tested and built simultaneously, according to the DoD, and improves "customer outcomes and mission value by automating, monitoring, and applying security at all phases of the software lifecycle: plan, develop, build, test, release, deliver, deploy, operate, and monitor".

A mission defence team specialist monitors cyber threats at the Niagara Falls Air Reserve Station, New York, on 8 February 2020. The cyber-security market is being altered by the evolution of artificial intelligence and machine learning. (USAF/Peter Borys)

1766968

McFadden said GDIT is working to harness new technological trends for its defence customers, for example through a modular system of cyber-security capabilities. “The modules can be deployed as a complete ecosystem or individually to fill cyber-security capability gaps,” he said. “The major capabilities provided by the ecosystem are network security, endpoint security, security event analysis, credentials management, security assessment, orchestration, automation, and threat intelligence.”

Gillett said that devices like software-defined radios are driving change in CEMA and supporting greater adaptability to future threats, particularly when combined with open standards for software development. He also said the market is being affected by the evolution of artificial intelligence (AI) and machine learning (ML).

“We see AI and ML being principally used initially in reducing the burden on individuals to triage through huge amounts of data related to cyber and CEMA, freeing them up to focus on the aspects of real interest,” he said. “We also see the growing need for processing and analytics at the edge [on or close to the sensor] in order to provide early indicators and warnings and to ensure that only the data of value is backhauled and moved elsewhere in the business.”

Complex domain

The ability to conduct joint force operations in CEMA environments is critical to national defence, particularly in an era of great power competition, said Chris Valentino, vice-president of information warfare and cyber survivability at Northrop Grumman. He said the company has worked with various military customers in the United States and internationally to "ensure our customers can control and defend information flow on the 21st century battlefield". "With access to advanced agile mission systems, defence forces can sense, share, decide, and act faster than adversaries, and with greater assurance," he told *Jane's* .

Valentino also highlighted the growing importance and utility of DevSecOps, along with 'agile' software development methodologies that aim to build software through an incremental and collaborative process between developers and customers that evolves over time. He pointed to the company's work as the system co-ordinator on the US Air Force's (USAF's) Unified Platform programme, which will support defensive and offensive cyber operations alongside cyber intelligence, surveillance, and reconnaissance (ISR) for US Cyber Command (USCYBERCOM). Northrop Grumman also works on other services for the command, from cyber command and control to mission training environments.

The recognition of cyberspace as the 'fifth operational domain' alongside land, sea, air and space opens up new battlefield scenarios "in which attacks, performed on the web or on the electromagnetic spectrum, can destroy national systems, manipulate or interfere with their critical information systems' operations and even cause real, physical consequences", said a spokesperson from Italy-based A&D company Leonardo.

Digital infrastructures are becoming more complex, comprised of various types of equipment and software, communication protocols, cloud applications, and other technologies and services, the spokesperson added. This complexity, and the growing number of connected systems and networks at national and international level, is combined with a growing need to share data and information, as well as the opening of military IT and operational technology (OT) systems to open-source technologies.

These various trends lead to an expansion of the attack surface of networks and defence systems, increasing vulnerabilities and fuelling the exponential growth of cyber attackers' weapons and tools, the spokesperson said. Attackers are attempting to launch complex and hybrid co-ordinated actions combining soft- and hard-power attacks, while many attacks involve combinations of state and non-state actors.

"The attackers are becoming increasingly aggressive," the Leonardo spokesperson said. "They are generating more and more sophisticated attacks and often conduct operations in order to differentiate targets and results in a way that is really difficult to predict or anticipate." There is thus a growing demand for more comprehensive cyber-awareness products and services from defence customers, the spokesperson added.

Such products and services must be augmented by emerging, disruptive technologies like big data and augmented reality, with the spokesperson drawing attention to the importance of AI, which can analyse huge volumes of data through deep learning algorithms. Leonardo has focused on using

such technologies to measure the impact of cyber risks, the spokesperson said, aiming to determine the actions a customer will need to take to neutralise cyber attacks and minimise their consequences.

The Falcon 9 Starlink rocket lifts off at Cape Canaveral Air Force Station, Florida, on 29 January 2020. There has long been a focus on cyber attacks that could take control of a satellite, including through a malicious software update. (USAF/Airman 1st Class Zoe Thacker)

1766969

Space focus

In a context of rapidly evolving technologies, defence specialists like GDIT must be "forward looking to address future threats related to IoT, 5G, quantum", and other areas, said McFadden. He also highlighted the development of new or quickly evolving markets for cyber security such as the space domain, the relevance of which has been shown by the establishment of the US Space Force and the growing commercialisation of space.

Cyber security in the space domain is also a major focus for Lockheed Martin. Ethan Puchaty, chief cyber architect at Lockheed Martin Space, noted that cyber security in space is not a new concept. For example, there has for some time been a focus on attacks that could take control of a satellite, including by changing its mission through a malicious software update. Denial-of-service attacks that prevent access to a system could also affect space assets, Puchaty added.

However, space was not viewed as a truly contested domain from a cyber perspective until recent years, Puchaty said. Lockheed Martin's cyber-space team is fairly new, as is Puchaty's, even though the company has worked on the cyber aspects of space equipment in a few cases.

There are several characteristics of space-focused cyber security that make it unique within the marketplace, according to Puchaty. “We can’t bring [the satellites] back down again to make changes, which really presents a number of challenges from an engineering standpoint in terms of how we keep up with threats and vulnerabilities as they evolve,” he said. This creates a demand for more software-defined approaches that have greater adaptability.

The environment also affects the technology. Puchaty noted that the orbit of a satellite can expose it to high doses of radiation, demanding components that withstand such an environment. “Those radiation-tolerant components are typically not as advanced or new as those that you find on the ground,” he said, which creates further cyber-security problems.

Puchaty’s team also incorporates lessons from the space domain into other areas of cyber security. Giving one example, he noted there has been an increased demand for cyber security around defence supply chains, which are a rich area of attack for adversaries who could maliciously modify a part or steal intellectual property. “It’s an area that we’re constantly concerned about and one that we’re putting a lot of effort into across the board,” Puchaty said.

Jon Check, senior director for cyber protection at Raytheon, underlined the need for adaptability in what is a quickly evolving sector in terms of technology and the demands of government policy. He said the DevSecOps approach brings advantages here, as it builds adaptability into software design.

“Because there’s a huge influx of dollars in the cyber market, there’s also a huge amount of innovation,” he told *Jane’s* . “How do we take advantage of that in a way that benefits our customers? DevSecOps allows us to ensure that we’re responding to policy changes and developing solutions that have security built in from the very beginning.”

An Advanced Extreme High Frequency 5 (AEHF-5) encapsulated satellite mated with an Atlas V launch vehicle rolls out in preparation for launch at Cape Canaveral Air Force Station, Florida, on 6 August 2019. Space has only recently been viewed as a contested cyber domain. (US Space Force/Van Ha)

1766971

Back to basics

While the military domain faces severe cyber security threats from state actors and other high-level adversaries, Check stressed the ongoing importance of routine 'cyber hygiene' that all organisations must pursue. He added that there remains a strong requirement for processes and systems that defend against malware, highlighting ransomware, where an adversary holds a victim to ransom by denying access to a user's network or threatening to expose data unless they pay a fee.

Military operators are just as vulnerable to 'phishing' attacks, where the adversary gains access to systems through tricking the user into clicking on a malicious link, as those in other sectors. There is therefore an ongoing demand for technology "that will see that type of behaviour and recognise something unusual", Check said. "Adversaries are very creative now with what they can do with data, even potentially changing your existing data by manipulating what you have on your network."

Raytheon's cyber-security business has transformed to change the way the company brings advanced products and services to market, said John DeSimone, vice-president of cyber security and special missions at Raytheon Intelligence, Information and Services. This aims to speed the delivery of commercial innovations, he told *Jane's* , boosting efficiency and staying ahead of the threat in real time.

As part of this the company has launched a new approach to securing enterprises, said DeSimone, called 'cyber as a service'. This approach provides virtual cyber support, security operations training, proactive threat hunting, managed detection and response, and several other services.

"Most breaches are designed to impact data in a variety of ways and, because of the nature of data, it is vulnerable through many layers of its life cycle across networks," DeSimone said. "We are taking action to address this threat and help organisations implement zero-trust environments, which protects data and verifies identities at every step of its life cycle."

Training demands

Training is a growing focus for Raytheon and the military cyber market. For example, the company is bidding for the US DoD's Cyber Training, Readiness, Integration, Delivery and Enterprise Technology (Cyber TRIDENT) contract, with a request for proposals expected later in 2020. Cyber TRIDENT aims to scale the military's Persistent Cyber Training Environment (PCTE) platform to support cyber training for all military elements, the environment being a cloud-based training platform that provides training for the DoD's Cyber Mission Force from the individual level to broader exercises.

The training domain is unique in the cyber domain because it is focused on an area that evolves so quickly, said Don Bray, director of cyber training at Raytheon Intelligence, Information and

Services. This means providers and operators must maintain constant contact with the cyber environment to keep up with changes.

“This is a man-made domain and it changes all the time, from an adversary’s perspective and your own standpoint in terms of defences,” he told *Jane’s* . “Every time there’s a new software release or a new patch, you’re actually changing the domain, so it’s in constant evolution.” The trend towards agile software and DevSecOps is of great importance here, he said, “so you always have the ability to change rapidly with the environment”.

Skills shortage

There is a much higher level of basic training in security awareness being rolled out across operators in different areas, said Gillett. BAE Systems is recruiting people with more diverse employment backgrounds and experiences than before and the company has established several academies to address in-demand skillsets in areas of specialist software development and electromagnetic activity.

“These accelerated courses, run in small groups, aim to get people starting work quickly on starter projects to build their experience,” Gillett said. He added that the UK skills base for cyber security in defence has grown markedly in recent years as a result of several government and industry initiatives. A similar, national-level government and industry intervention could help stimulate the electromagnetic activity skills base, he added.

US National Guard soldiers in a lecture during the training portion of the 'Cyber Shield' exercise at Camp Atterbury, Indiana, on 8 April 2019. The biggest problem facing cyber security in defence is finding people with the right skills. (US National Guard/Spc William Phelps)

1766972

The biggest demand ADS has seen in the rise of cyber security and technologies is for people with the right skills, noted Everitt. This is tied into wider shortages associated with science, technology, engineering, and mathematics (STEM) disciplines. "The biggest theme we see is about how we attract people into the sector who know how to work with the technologies, especially when the defence sector is competing with commercial areas of cyber," Everitt observed.

It is a good sign that more people are discussing the skills shortage, said Check, with the problem becoming a major topic over the past two years. Although there have been a wide range of activities promoting cyber and STEM careers, he warned that the benefits will not be realised for some time, noting that staff also need years of on-the-job experience before they can be truly proficient.

Advances in AI could help address the skills shortage, Check added, with automated algorithms increasingly able to handle tasks that would previously have been addressed by human operators. Check emphasised the ongoing need for people in a range of higher-level roles, despite noting there is a strong case for people to still be given positions in areas that might be more easily automated.

"We still need certain areas where people can grow and gain the experience to become subject matter experts," he said. "We can't just hire senior-level people because, without the entry-level roles, where are the senior people going to come from? They don't just magically appear."

Commercial potential

As with many other areas, defence companies often look to the commercial sector for technology and products that may be better and cheaper than the ones already produced within the military domain, Everitt noted. "Looking elsewhere also means that we may be able to draw on different technologies to make us more efficient," he said.

There are also increasing opportunities for small and medium-sized enterprises (SMEs) in the cyber security domain. "As the market is growing so quickly, SMEs prove more agile to respond to emerging technologies and utilise them for cyber capabilities," Everitt said. "What we then see is SMEs proving of greater value to primes who look to advance their capabilities in the area."

Raytheon is increasingly tapping commercial innovations to build broader cyber-security products and services, said DeSimone. The company has formed partnerships with several commercial companies that offer sophisticated technology with agile delivery models, including with SMEs. These companies "offer advanced capabilities for protection of critical infrastructure, analytics, data orchestration, and insider threat protection, just to name a few", DeSimone noted.

Gillett said that advances in AI and cloud hosting are being driven by adjacent sectors but also offer huge benefits to defence, adding that BAE Systems is adopting these advances. He also highlighted an area that is not perhaps commonly associated with cyber security: climate change. "We are starting to see mention of this now [in defence]," he said. "We are looking at ways cyber can

reduce travel requirements for better logistic supply chain management."

A Yuneec Typhoon H rotary-wing UAV hovers above a Stryker Infantry Carrier Vehicle at the 'Cyber Blitz 19' exercise at Joint Base McGuire-Dix-Lakehurst, New Jersey, in September 2019. The exercise informed the US Army about how to perform evolving CEMA across operations. (US Army/Edric Thompson)

1766970

Cyber security is a unique military domain, with defence companies not just acting as suppliers of high-end technology, but also being forced to defend themselves as targets, with various actors seeking to steal their valuable information or damage them because of political or economic motivations.

"Our cyber commitment to our customers mirrors our commitment to internal operations, ensuring we have the cyber protection for today while anticipating the threats of tomorrow," said McFadden. "Our internal responsiveness and resilience to current threats and anticipating future risks are imperative."

Check said Raytheon sought to use its own experiences and knowledge gleaned from defending itself against cyber attacks to inform its offerings for its customers. This can be beneficial from a business perspective, he said, as the company can use itself as a real-life case study of how certain techniques or technologies can bring benefits.

"We can say that here are the lessons we have learned at Raytheon; here's what it takes for us to defend ourselves and maintain our posture," he said. "In defence we take that very, very seriously."

Comment

Cyber security is not a new domain, but its growth as a military focus in recent years is undeniable. As it reaches across military programmes and areas of technology, it can be difficult to pick out key factors. However, several issues are high priorities for industry practitioners.

There is a clear effort to grasp the opportunities and understand the problems posed by the growth of cyber security in new domains, as exemplified by the efforts in the space sector. Companies are looking to the future of training and assessing their own cyber security defences. There are also questions being raised over the potential of AI, in terms of its ability to bolster cyber-security defences and its usefulness in a market where qualified employees are hard to find.

This last aspect looms across the military cyber domain: the task of getting enough suitable staff. This is a problem for all STEM-related businesses, but perhaps particularly in defence, which must compete with the commercial domain for a limited pool of employees. Many in the industry, government, and beyond will be carefully assessing the various efforts across Western nations to expand those pools of suitably experienced cyber-security practitioners.