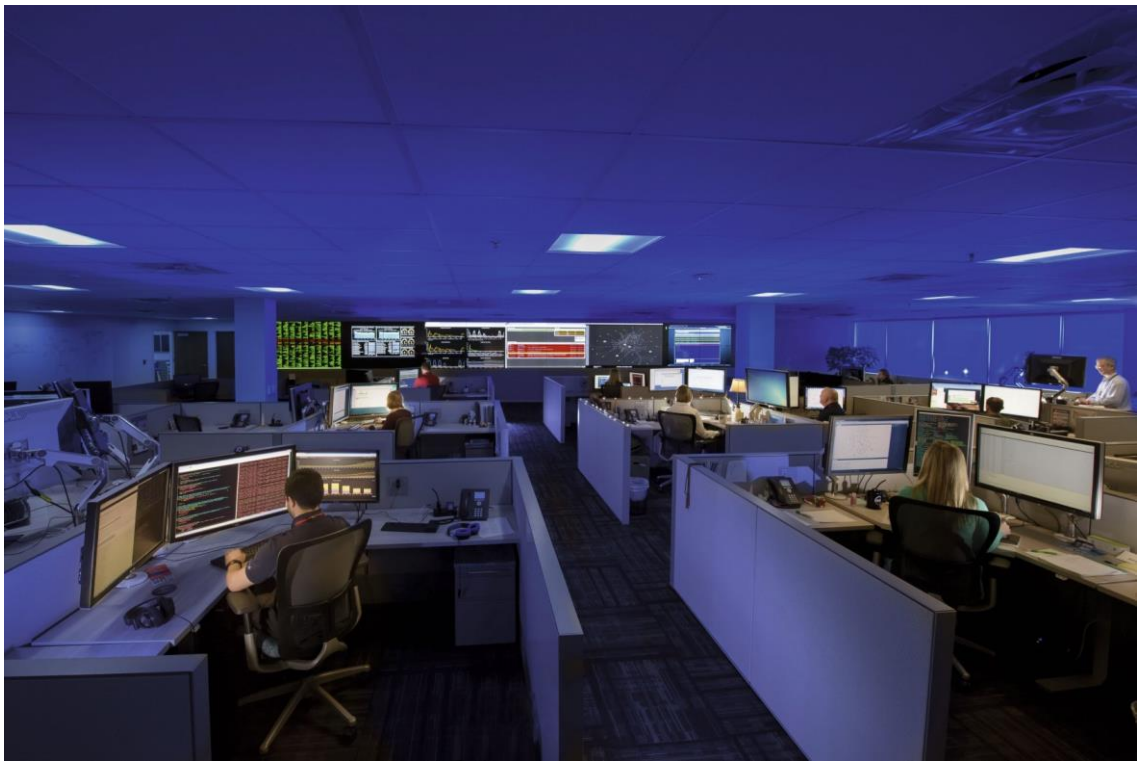
The fifth domain: Cyber security challenges and opportunities

Cyber security has emerged as a priority for military organisations during the past decade, gaining it the label of being the 'fifth domain' of warfare. This has driven a surge of interest among defence suppliers, from smaller, specialist operators to the major primes. *Gerrard Cowan* reports

There are challenges and opportunities in the cyber domain that are arguably unique to defence companies. This is partly driven by the diffuse nature of the threat, with potential adversaries, ranging from state actors to criminal gangs, posing a danger to military systems and networks, according to Esti Peshin, head of cyber technologies at Israel Aerospace Industries (IAI). "It is difficult – and unwise – to attempt to separate the military and civil aspects of the threat in a clean fashion," she warned. For example, a military platform could suffer an attack from a non-military source, while a major attack on critical national infrastructure, such as an energy network, could be considered an issue for civilian and military forces alike.



Some of Lockheed Martin's cyber intelligence analysts at work. Defence companies are increasingly focused on cyber security as a business area, but it is also a priority for them as users. (Lockheed Martin)

1726020

The cyber sphere is an ever-changing domain from a defensive and offensive perspective. "It's like an arms race, but it's an arms race at two speeds," Peshin told *Jane's* . "The bad guys are constantly

searching for vulnerabilities and developing attacks; the good guys are constantly trying to counter this."

The domain is always evolving, Peshin explained, so suppliers like IAI are seeking to make their systems and services as adaptable as possible to keep up while also searching for potential weaknesses in a rapidly changing suite of systems and technologies. For example, she pointed to the growing interest in the 'Internet of Things' – through which a whole range of battlefield systems could be connected to a network, as well as civil systems – and the roll-out of 5G network technologies.

"I don't know if there are any vulnerabilities in these technologies, but I assume there are – because there are vulnerabilities in everything," she said. "The bad guys are looking at it from the perspective of how to exploit this network and the good guys are looking at how to protect it. Everything is moving very, very quickly."

Part of the challenge is defining what 'cyber' means, noted Dave Woolrich, programme manager for cyber warning at BAE Systems, adding that the term is used to cover a wide range of threats and technologies.

"What does being secure mean?" he asked, "And how do you implement that as a performer in the industry? There are definitely challenges around that."

The approach taken by BAE Systems has been to work to defend against entire classes of threat, rather than individual ones, explained Sam Hamilton, chief scientist for the BAE Systems FAST Labs Cyber Technology Group. This could be particularly useful for protecting a platform that is unlikely to undergo frequent maintenance and so would not receive patches to update against the latest individual attacks on a regular basis.

"If you have a deployed vehicle that is not frequently going through maintenance cycles and is purposefully kept off the network, you're not going to be able to update it regularly," he argued, "so we can't have a model where you're required to upgrade with new defences weekly or daily".

A solution to this is to characterise the behaviour of entire classes of attack so that, even if an individual attack represents "a new way to infect the system", it is still likely to be part of a broader class and can still be detected. This substantially reduces the work involved for companies and militaries, Hamilton explained, and cuts back on the potential for surprises.

Though once viewed as something separate or standalone, the cyber domain is now taken account of within the requirements for virtually all new defence platforms, said Rear Admiral (retd) Bill Leigher, director of Government Cyber Solutions for Raytheon. Although network defence has been a priority since the 1990s, the increasing use of software, processors, and networks on individual platforms means they "have weaknesses that may be exploited by an adversary", he noted.

At the same time Leigher noted that the United States and its allies are using the knowledge gathered by companies like Raytheon to collect intelligence. "If you want to understand cyber defence," he explained, "then you have to also understand how to attack systems: where the weaknesses are and how to take advantage of those vulnerabilities". This is at the core of Raytheon's strategy for cyber defence, he added.

"The two sides go hand in hand," he said, noting the continuing evolution "from what 20 years ago was just about the network and now includes every piece of software and every processor on the battlefield".

Civil partners

Defence contractors are not alone in supplying cyber systems and services to the United States and other militaries. Names that are more familiar in the civil world have also boosted their cyber defence businesses in recent years. The US computing giant IBM, for example, conducts cyber-security work across the US armed forces and those of other countries, said a spokesperson for the company.

One of the company's major focuses is its work with the US Army's Logistics Support Activity (LOGSA), to which IBM provides risk management framework (RMF) security controls to the organisation's IT enterprise. The company's work with LOGSA is aimed at shrinking the logistic organisation's overall IT footprint to make it more efficient and to increase security.

"We've used that model to encourage other DoD [US Department of Defense] customers and have performed similar work for them," the spokesperson said. "We look at how their IT infrastructure is designed and configured, and where we can apply technology or process improvements to boost their security posture."

Given that the cyber threat is continuously evolving, one of the advantages of RMF – the information security framework for the US federal government – is that it provides a solid foundation for cyber defence while at the same time being able to be continuously upgraded. The spokesperson described how RMF is built on technical and process-related controls, from firewalls and switches to ensuring that system administrators receive appropriate oversight.

"Once you get that strong foundation, it allows you to do the continuous monitoring and protection but also to insert some emerging technologies into your cyber framework," the spokesperson explained. "It starts with having a good, solid foundation. If you're constantly on the defensive and dealing with network attacks, then you don't have the resources and the time – and in some cases the vision – to evolve your security environment and security ecosystem."

[Continued in full version…]

(1034 of 3548 words)