LORCA NEEDS ACCELERATOR: DEFENCE

LORCA

Cybersecurity has become mission-critical when it comes to national security.

In 2016, NATO recognised cyber as the fifth domain of warfare in addition to land, sea, air and space. And, given that they're cheaper to carry out than traditional warfare, the frequency of publicly reported state-sponsored cyber attacks is increasing every year.

To understand the changing nature of the challenge, LORCA brought together cybersecurity experts, members from our programme and some of the most influential people in the sector.

HELD UNDER THE CHATHAM HOUSE RULE, OUR DISCUSSION UNVEILED A RANGE OF INSIGHTS, CHALLENGES AND OPPORTUNITIES.

01

The sector recognises the benefits of collaboration but has concerns about revealing sensitive national security vulnerabilities

02

Alignment between home and deployed cyber operations is desirable

03

Supply chain security is a challenge, while hackers are armed with more information on supply chains

04

The sector could be unknowingly buying counterfeit components

05

Tackling disinformation is a job for both the defence sector and social media

06

Public education is needed to combat disinformation

07

Legacy infrastructure is making some attacks easier

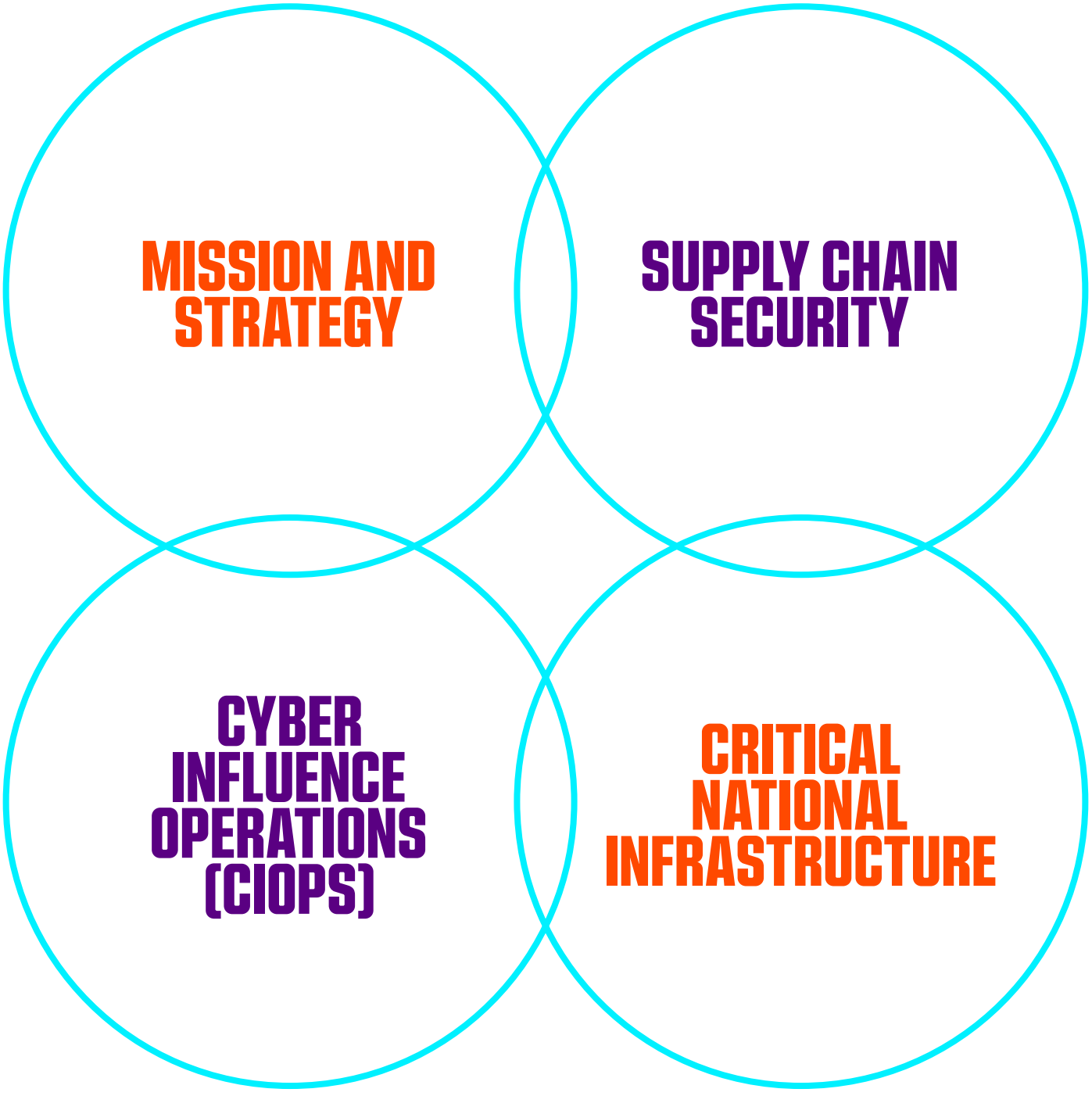
08

More collaboration and information sharing is needed to secure CNI in particular

09

Understanding the CNI threat landscape is a challenge, which makes intelligence sharing even more important

INSIGHTS, CHALLENGES AND OPPORTUNITIES.



MISSION AND STRATEGY
THE SECTOR RECOGNISES THE BENEFITS OF COLLABORATION BUT HAS CONCERNS ABOUT REVEALING SENSITIVE NATIONAL SECURITY VULNERABILITIES.

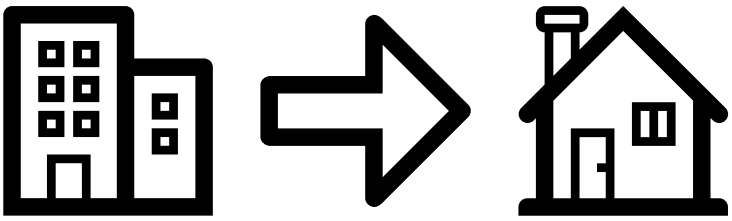
Organisations are still reluctant to share information that could reveal critical vulnerabilities in a nation's cyber capability"

Cyber attacks against national organisations and critical national infrastructure are managed by individual defence organisations, but participants felt there was an opportunity for a cross-section of the sector – not just a selection of individual organisations – to collaborate more deeply and share information.

This could help the sector understand the nature of the threat better and actively hunt threats more effectively, which could reduce Advanced Persistent Threat (APT) dwell times.

But despite these potential gains, organisations are still reluctant to share information that could reveal critical vulnerabilities in a nation's cyber capability. This is one of the main reasons why the defence sector is more reliant on intelligence from the private sector.

MISSION AND STRATEGY ALIGNMENT BETWEEN HOME AND DEPLOYED CYBER OPERATIONS IS DESIRABLE.



More emphasis on cyber operations when deployed rather than when at home"

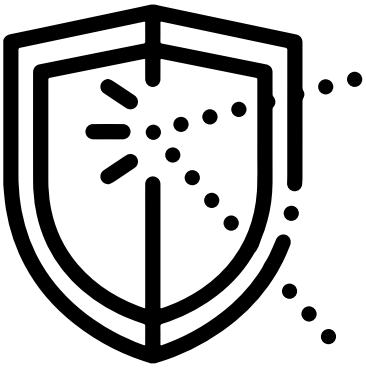
Attendees highlighted that there is more emphasis on cyber operations when deployed rather than when at home. This has caused some separation between priorities and strategy.

Overall, there should be more focus on looking at cyber operations and strategy as a whole for both deployed and home operations to ensure that priorities and strategies are aligned.

SUPPLY CHAIN SECURITY

SUPPLY CHAIN SECURITY IS A CHALLENGE. MEANWHILE, HACKERS ARE ARMED WITH MORE INFORMATION ON SUPPLY CHAINS.

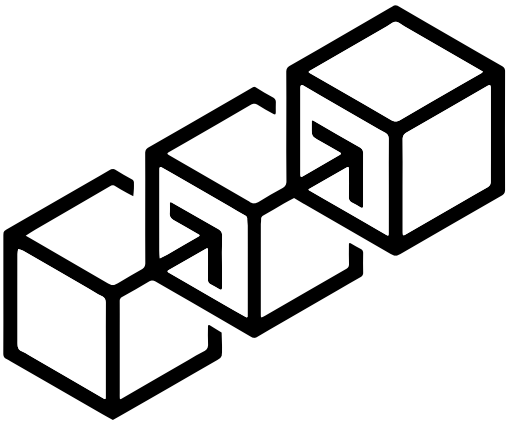
The defence sector doesn't have full visibility of its supply chain"



Globalisation has resulted in longer supply chains, with each supplier managing their own supply chain and potentially sharing highly sensitive information. This means the defence sector doesn't have full visibility of its supply chain, which poses a national security risk.

At the same time, threat actors now have a better window into the vulnerabilities in the sector's supply chains. Many organisations are moving to commercial off-the-shelf software to manage their supply chains, but security vulnerabilities in this software are continuously being discovered and commonly circulated in the public domain (where they can be exploited more easily than if a custom-built, in-house application was being used).

SUPPLY CHAIN SECURITY
THE SECTOR COULD BE UNKNOWINGLY BUYING COUNTERFEIT COMPONENTS.



Finding replacement components that manufacturers have discontinued can be hard”

Defence hardware systems are designed for long-term service – some might be used for over 40 years – and finding replacement components that manufacturers have discontinued can be hard.

Procurement departments under pressure may then source parts from less reputable sources – and unknowingly buy a counterfeit chip with security flaws.

CYBER INFLUENCE OPERATIONS TACKLING DISINFORMATION IS A JOB FOR BOTH THE DEFENCE SECTOR AND SOCIAL MEDIA PLATFORMS.

Cyber warfare of the future may be less about hacking power grids and more about influencing views to shape the political environment. Using techniques like disinformation campaigns, the goal of Cyber Influence Operations (CIOps) is to cause confusion, distraction, division and demoralisation while complimenting operations in the four conventional domains of land, sea, air and space.

Given its ability to interfere in a nation's social and political affairs, action needs to be taken at a national level"

Creating false profiles or deepfakes on social media is a popular method of spreading disinformation and mobilising people politically. It's a method used both by foreign intelligence service operations to influence opinion or destabilise another country, as well as domestic actors who want to rally their own citizens against their enemies.

Attendees discussed how deepfake videos of politicians and public figures could be altered to change the narrative, and then distributed through false personas on social media.

There's an ongoing debate about what responsibility platforms have to detect and remove fake news, but our attendees wanted to see a more coordinated approach between national intelligence services and social media platforms to tackle this issue. But, given its ability to interfere in a nation's social and political affairs, action needs to be taken at a national level and the onus isn't entirely on social media platforms.

Attendees highlighted the fact that while social media platforms enable messages to spread instantly and globally and have a duty of care to their users, there are complications around establishing if posts are genuine and accurate.

Techniques exist to detect deepfake videos, but the challenge is integrating this with social media platforms to flag suspected fakes. There are also questions around whether removing posts deemed to be fake news could amount to censorship in some cases.

CYBER INFLUENCE OPERATIONS PUBLIC EDUCATION IS NEEDED TO COMBAT DISINFORMATION.

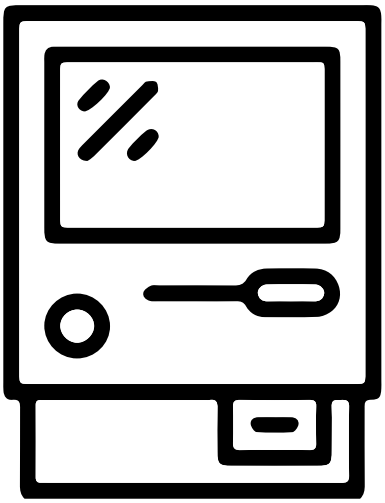
We need to do a better job of educating the public. This should cover everything from fake profiles and deepfake videos to fake news."

Attendees discussed how the vast majority of people are unaware that they could be the target of foreign intelligence service operations who want to distribute political narratives.

And, given what's at stake and how difficult it can be to tell what's real and what's fake in deepfake videos, attendees think we need to do a better job of educating the public. This should cover everything from fake profiles and deepfake videos to fake news.

CRITICAL NATIONAL INFRASTRUCTURE

LEGACY INFRASTRUCTURE IS MAKING SOME ATTACKS EASIER.



Critical National Infrastructure (CNI) includes assets that are essential for the functioning of a society and economy, whether it's a chemical plant, a communications network, defence facilities, health services or water supplies.

A cyber attack on these affects people's physical security, public health and the economy as a whole.

CNI relies heavily on industrial control systems and operational technology that was developed decades ago with a focus on resilience, performance and safety – with little provision for security.

It's relatively easy to carry out attacks on these legacy networks, which focus on reconnaissance or disruption and sophisticated man-in-the-middle attacks (where two parties think they're communicating directly but somebody is listening in or altering the data).

CRITICAL NATIONAL INFRASTRUCTURE MORE COLLABORATION AND INFORMATION SHARING IS NEEDED TO SECURE CNI IN PARTICULAR.

Although attacks on a country's CNI can be considered acts of war, the lack of physical boundaries and the fact that the infrastructure is owned and managed by organisations (rather than the military) makes it hard for the military to detect breaches and intervene.

Attendees called for more collaboration among the CNI community (including manufacturers). As a community, they should share knowledge and take collective responsibility for protecting CNI.

Attendees discussed how suppliers like Siemens are considering sharing technical information about their solutions to help others in the industry learn more about their systems. This openness would open up new opportunities to learn about the CNI environment and encourage innovation that protects it.

> *"Openness would open up new opportunities to learn about the CNI environment and encourage innovation that protects it"*

CRITICAL NATIONAL INFRASTRUCTURE

UNDERSTANDING THE CNI THREAT LANDSCAPE IS A CHALLENGE, WHICH MAKES INTELLIGENCE SHARING EVEN MORE IMPORTANT .

A constant challenge is having full visibility of all assets and endpoints within CNI. Having legacy systems in place adds extra complexity. Organisations using legacy systems tend to have complex security architecture, where legacy systems have been web-enabled without proper asset inventory or decommissioning. This makes it difficult to know what is and what isn't connected to the internet.

And since the equipment and systems used in CNI tend to be bespoke, it's hard to have an accurate understanding of the vulnerabilities and threats using conventional threat intelligence sources.

Using honeypots to deploy fictitious networks and assets could be a useful method of gaining intelligence specific to an attacker and the vulnerabilities they were trying to take advantage of. Sharing this sort of intelligence with the wider community could help private sector innovators develop solutions that identify and stop threat actors earlier, protecting CNI.

> ***"It's hard to have an accurate understanding of the vulnerabilities and threats using conventional threat intelligence sources"***

CONCLUSION: TOWARDS A COLLABORATIVE FUTURE.

Technology is changing the nature of warfare rapidly, and our defence sector's needs are evolving.

As our Needs Accelerator showed, the sector is keen for more collaboration with manufacturers, government departments, academia, infrastructure bodies, the media and private sector innovators. National security is a collective responsibility.

Leading voices also recognise the wide-ranging impact cyber threats can have, whether it's to destabilise a nation by causing confusion or creating an environmental crisis by targeting national infrastructure.

But while there's clearly a desire to deploy new cyber solutions, our attendees spoke about challenges such as a lack of intelligence sharing (given the sensitive information involved).

Some areas, such as tackling the spread of disinformation, also throw up complex questions around where the responsibility lies and how nation states or social media platforms can tackle the challenge without infringing on free speech.

There are clear opportunities for innovators to grasp – especially when it comes to enabling secure collaboration and information sharing, securing the supply chain, information sharing to defend critical national infrastructure and educating the public about fake news techniques.

“

There are clear opportunities for innovators to grasp – especially when it comes to enabling secure collaboration and information sharing, securing the supply chain, information sharing to defend critical national infrastructure and educating the public about fake news techniques.”

CONNECT WITH US

lorca.co.uk
info@lorca.co.uk

Twitter: @LORCACyber
LinkedIn: LORCA Cyber

FIND US

Plexal, The Press Centre
Here East, 14 East Bay Lane
Queen Elizabeth Olympic Park
London, E20 3BS

LORCA