Photo courtesy of Shutterstock

Beware 'the new Trojan Horse': Why cyber hardening is imperative to government defence

Based in Ornsköldsvik, Sweden, Clavister AB supplies communication service providers, governments, enterprises, and managed security service providers in more than 150 countries with virtual cyber security and digital threat deterrence software. The company's Cyber Armor solution provides military vehicles with embedded defence against cyber-attacks, regardless of their origin.

Stefan Brodin, Head of Defence, Clavister

Ruse de guerre – or ruse of war – is a term that refers deceptive or creative and unorthodox means in the act of battle. From the Greek's deployment of the Trojan Horse c.1400 BCE to Britain's inflatable tanks in World War II, triumphant victors have emerged through their ability to be both cunning and innovative.

The time is now to keep your defences up to scratch

In the present day, the need for ruse de guerre still stands. At a time when technology is at the forefront of defence equipment, the landscape is both smarter and more connected than ever. However, with greater technological advancement comes greater risk. The potential for cyber espionage and wide-scale damage is elevated and we must do everything we can to limit detrimental effects. Historically, innovation has reshaped the operational domains of the defence space, with military powers utilising the newest inventions possible to strengthen their forces. As the cyberbattle space emerges, the need for cyber strength is critical. Adaptation and innovation are key to harnessing this.

Imagine a race car with all the latest technology to perform best on the track. While it is designed to go the fastest, it has not been designed for the purpose of standard road use. Now think of military-grade vehicles that have every technology available to perform the best in warfare, from strategic mapping to AI-powered risk analysis and identification. What they do not have is cybersecurity at the centre of the design process. Although it's easy to think that sheer defence power without these other factors makes for the best vehicle, it's fundamental that military vehicles aren't 'one-trick ponies' and that complacency has no place in the defence space. Making sure that every system and network in the vehicle is protected from threats, both visible and invisible, is essential.

Preventing the defence space from becoming a playground for cyber-attacks

We're looking at a situation in which the possibilities for smart human interference by way of a cyber-attack are not only endless, but also possess the potential to degrade overall military capacities. Currently, it is the latter type of cyber operation that could have some of the most significant ramifications on the battlefield, rather than decisive military manoeuvres in their own right. There is an overwhelming likelihood that these scenarios will occur as the defence space develops and a multitude of different nations are in possession of increasingly sophisticated cyber capabilities.

The other related sector most at risk of being targeted by such threats is the supply chain. Vehicle manufacturing is dependent on a variety of different organisations and suppliers, with a cross-section of parties working across different aspects of the development of this complex machinery. Ultimately, the

CHOOSE YOUR OWN ADVENTURE

CREATE.
All things pre-production to post.

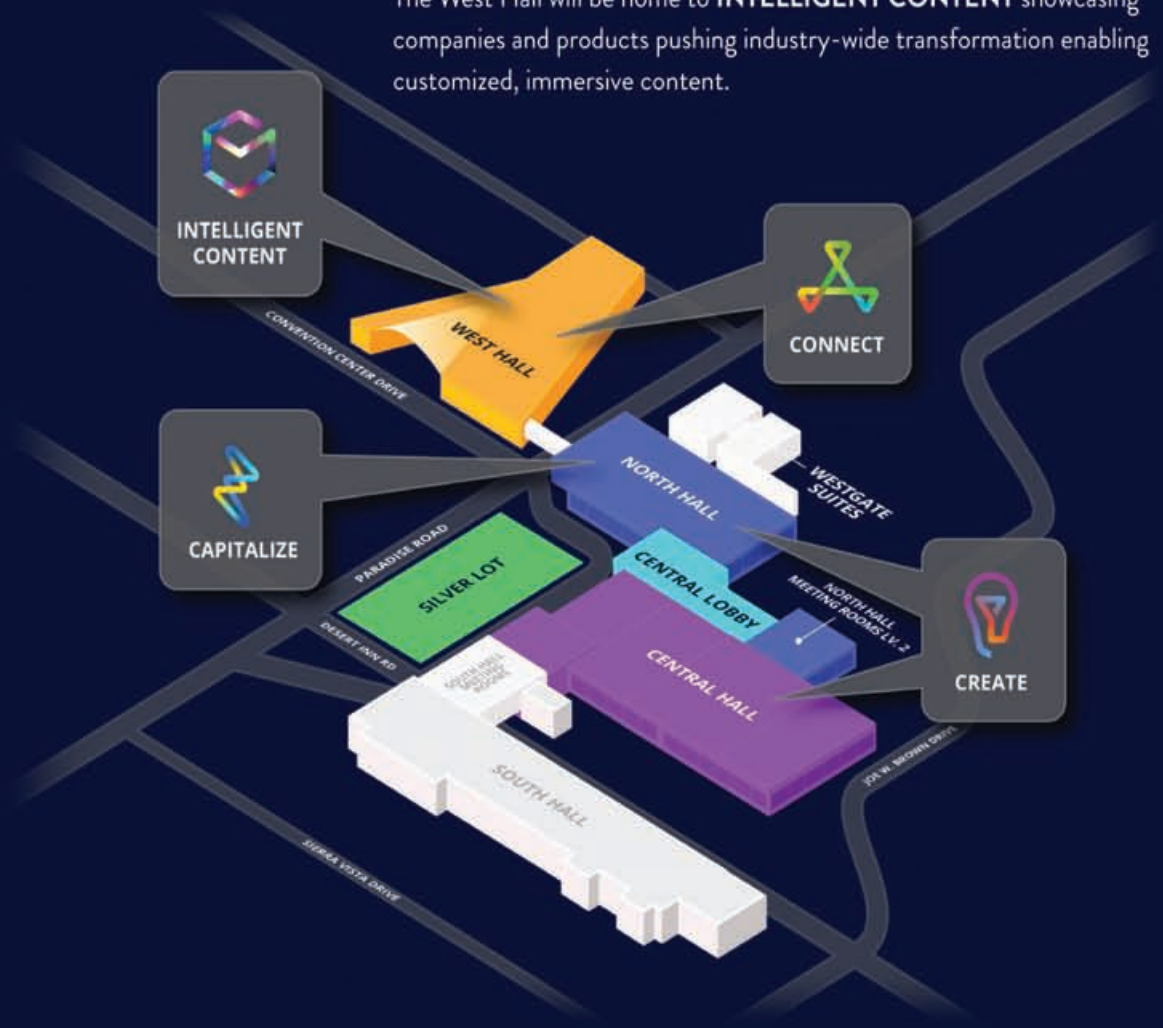
CONNECT.
All things distribution and delivery.

CAPITALIZE.
All things reach and ROI.

An entirely reimagined experience. The 2022 NAB Show opens on Sunday with four distinct show floor collections ramping your journey through the content lifecycle. Accelerate at will. Feel the rush of hundreds of exhibitors. High-caliber education. Best-in-breed products. Direct connections to peers and industry experts. Everything and everyone will be there (we just need you).

AND...SAY HELLO TO THE WEST HALL!

The West Hall will be home to **INTELLIGENT CONTENT** showcasing companies and products pushing industry-wide transformation enabling customized, immersive content.



NABSHOW®
Where Content Comes to Life

APRIL 23 - 27, 2022
EXHIBITS APRIL 24 - 27
LAS VEGAS CONVENTION CENTER
NABSHOW.COM | #NABSHOW

Stefan Brodin, Head of Defence, Clavister

more parties involved in these processes, the more scope there is for cyber loopholes and opportunities for espionage. A single armoured vehicle can be made up of components from hundreds of different suppliers. All it takes to threaten the entire construction process is a single weak link.

Knowing that the scope for attack is now broader than ever before, with adversaries demonstrating their capabilities to utilise threats to their advantage, we must act to ensure security at the earliest possible opportunity. We need only look at the number of attacks taking place in the supply chain at the moment, from the attack on Cape Town's main port last year having huge ramifications on international shipping to the Colonial Pipeline attack, which led to the USA calling a national emergency. These attacks are capable of both impeding the development of these tanks in the first place and targeting entire fleets of armoured vehicles. If an attack were to take place, the consequences could be perilous – from paralysing entire fleets to rendering crucial defences obsolete.

The solution: cyber hardening the past and the present

There is a solution to this point of vulnerability, and it's within our grasp. Cyber hardening can protect both new and legacy military platforms, as well as warfare systems. However, navigating the defence space involves carefully considering this new threat landscape. Unlike the commercial market, where businesses can work to their own timelines independently, defence requires cross-organisational collaboration, harnessing military expertise, the most up-to-date cybersecurity strategy, and cutting-edge academic research. Ensuring that military defences are up to scratch requires national and, in some cases, international efforts combining financial planning with research and development. Countries are now specifically charging their efforts towards cyber defence by increasing their budgets or directing specific investment towards it.

The UK is one example of this – it has announced a massive £16bn increase in spending, making evolving technologies a focal point – ensuring that AI and cybersecurity measures are harnessed to their full potential. As a result, defence corporations also are looking to cyber resilience as an integral part of their deliverables, working in alliance with several research programmes and think tanks to expand their offerings where possible and fill the current gap in the sector. One example of this is the Vinnova Funding project in Sweden, which is seeing the likes of BAE Systems working with others in order to enhance in-vehicle network security.

Working in partnership will determine the future safety of military vehicles

Acting in collaboration ensures that going forward, military vehicles – both those in development and legacy models – are fully assessed. Weaknesses can be pinpointed and the path to maximum security clearly established. While a tank may look tough as nails from the outside, there are internal weaknesses that can easily be exploited by adversaries, including weapon firing computers, external video cameras and sights, battle command systems, external sensors, communications systems, and digital engine control systems.

Using AI can help ascertain an unbiased overview of a piece of machinery and all its weak points. Not only will this drive future innovation, but also it will prevent any surprises that could otherwise have catastrophic implications. Where cybersecurity has previously been separated from defence development, and often thought of as an add-on on the side, seeing networks forming across the space can help ensure maximum protection.

AI can also help governments determine the pros and cons of using legacy vehicles and machinery from other countries. Having an objective overview of the potential of a machine and whether or not it can withstand current threats can help with evaluating budgets and full military potential. It could even one day save a nation from being caught out and ill-equipped to deal with the threat at hand.

Creating an air-tight strategy will put you in the strongest position

What's more, bringing cybersecurity strategy into a wider defence strategy will help to protect wider military networks in the long run. No longer will militaries have to be 'stuck between a rock and hard place' pitting the inefficiency of decentralised networks against overexposure to cyberwarfare. Instead, they can align all their goals for maximum protection, confident that they have a solution which can enable rapid response time and maximum damage control.

All these benefits can be further strengthened by making sure that tanks and other types of warfare machinery have the correct software installed into their systems. This way they will be able to detect encroaching malware. Having such software can form the basis of an intrusion detection system, which is a crucial step towards security. However, in choosing software, militaries and defence organisations need to consider whether they're selecting the right security for the occasion. Unlike other sectors and spaces, defence does not present the same attack vectors (such as ransom or financial gain). Instead, attackers will be looking to exploit weaknesses that can lead to greater vulnerability or redirect the balance of power.

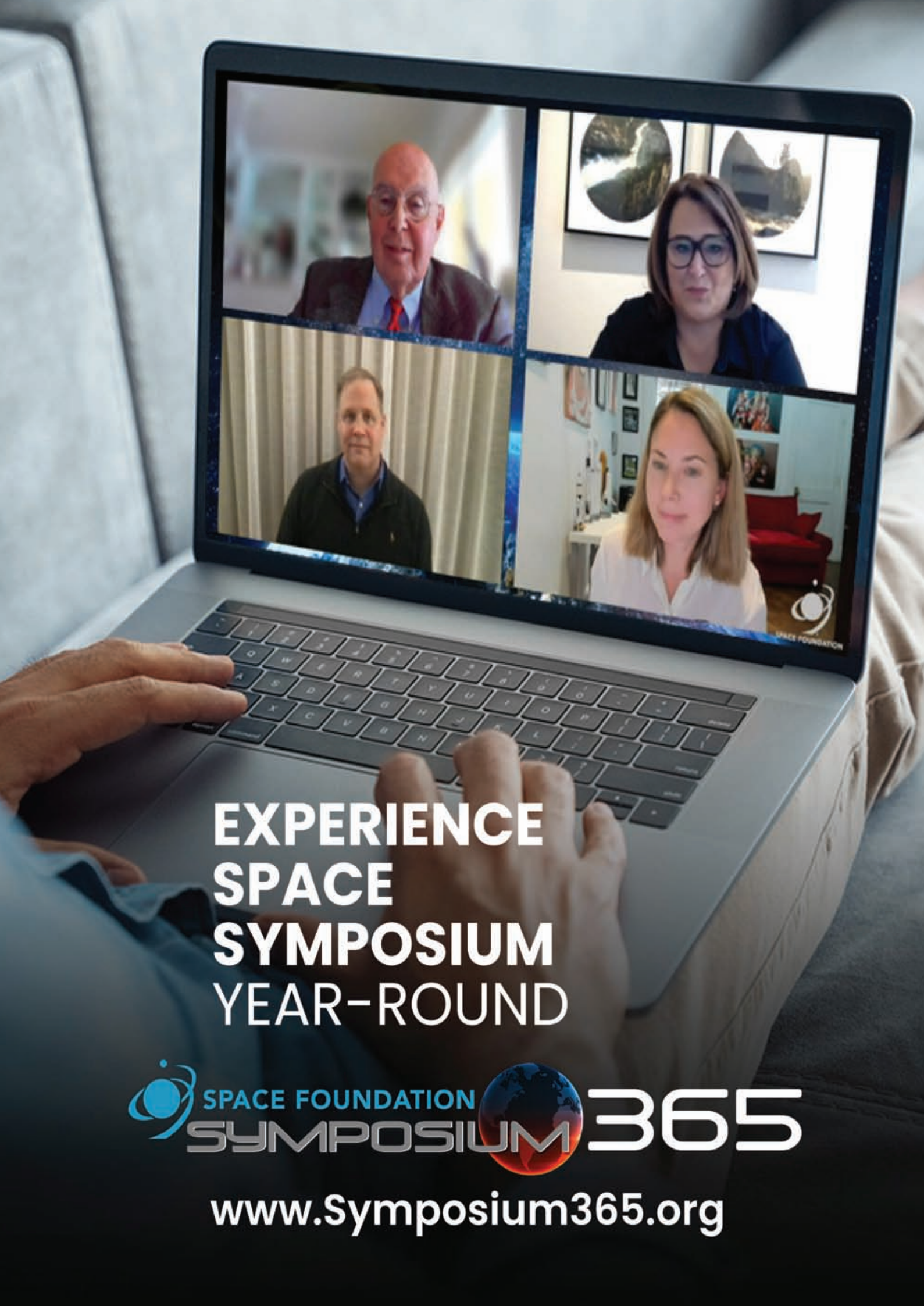
Therefore, the cybersecurity defences deployed must be tailored for the space, factoring in all aspects of a military vehicle that make it unique from other commercial means of transport.

Having a system that can scan and segment networks where necessary, separate components to assess vehicle health, and allow for authorised communication only, will all be key considerations.

The future lies with the people behind it

While the steps to maximising cybersecurity for defence vehicles have been outlined, making sure they are followed and adhered to is equally critical. The war is no longer limited to the battlefield. We now live in a world of hybrid warfare being fought on two fronts: in the field and behind a screen.

Installing the relevant software and defences is only half the solution – these changes also need to come from those operating the vehicles and leading the organisations. Making sure that personnel are well-trained and have all the skills they need to react correctly is key to achieving comprehensive protection. **GMC**


EXPERIENCE
SPACE
SYMPOSIUM
YEAR-ROUND
SPACE FOUNDATION
SYMPOSIUM 365
www.Symposium365.org