

# GMC

Linked in   YouTube

ISSN 1756-3240

February 2023

# Global Military COMMUNICATIONS

## Defending against cyber threats

New horizons for defense

Digital backbone

Q&A Rivada Space Networks



*Front cover photo courtesy of Bits And Splits/Shutterstock*

Sign-up now for your **FREE** digital copy...visit [www.globalmilitarycommunications.com](http://www.globalmilitarycommunications.com)





# COMTECH<sup>TM</sup>

## Fluent in the Future<sup>TM</sup>

At **Comtech**, we're building the future of hybridized connectivity, with technology that integrates **terrestrial and satellite communications networks**.

Relentless pursuit of a better way:  
empowering people to connect  
everything and everyone.

[www.comtech.com](http://www.comtech.com)



**Executive Editor**

Crispin Littlehales  
crispin@dsairpublications.com

**Associate Editor**

Laurence Russell  
Laurence@dsairpublications.com

**Marketing and Business Development**

Belinda Bradford  
belinda@dsairpublications.com

**Marketing Production Manager**

Jamaica Hamilton  
jamaica.hamilton@dsairpublications.com

**Circulation Manager**

Elizabeth George

**Publisher**

Jill Durfee  
jill.durfee@dsairpublications.com

**Publishing Director**

Richard Hooper  
richard@dsairpublications.com

**Managing Director**

David Shortland  
david@dsairpublications.com

No part of this publication may be transmitted, reproduced or electronically stored without the written permission from the publisher.

DS Air Publications does not give any warranty as to the content of the material appearing in the magazine, its accuracy, timeliness or fitness for any particular purpose. DS Air Publications disclaims all responsibility for any damages or losses in the use and dissemination of the information.

All editorial contents  
Copyright © 2023 DS Air Publications  
All rights reserved

DS Air Publications  
1 Langhurstwood Road  
Horsham  
West Sussex, RH12 4QD  
United Kingdom  
T: +44 1403 273973  
F: +44 1403 273972  
admin@dsairpublications.com  
www.globalmilitarycommunications.com

# GMC



● ● Defending cyber threats - page 8

## Contents ● ●

<b>News review</b>	<b>4/5/6</b>
<b>Q&amp;A Daniel Gizinski, Comtech's Chief Strategy Officer for Defense, Comtech</b>	<b>8</b>
<b>A digital backbone: how it strengthens and weakens national defence</b>	<b>12</b>
<b>Q&amp;A Ronald van der Breggan, Chief Commercial Officer at Rivada Space Networks (RSN)</b>	<b>14</b>
<b>Cybersecurity as a service: Enabling workers to withstand cyberattacks from the most remote of sites</b>	<b>18</b>
<b>Q&amp;A Simon West, Cyber Advisory Lead for Resilience</b>	<b>20</b>
<b>New horizons for the defence industry means the outlook is bright for 2023</b>	<b>24</b>



● ● If you would like to supply information for future issues of GMC please contact Crispin Littlehales

Photo courtesy Rivada Space Networks

# Airbus launches European Defence Fund R&D projects ●●

Airbus has launched two defence research and development projects that it is coordinating as part of the 2021 European Defence Fund (EDF). In July 2022, the European Commission selected, among others, eight collaborative projects that Airbus is part of, covering different innovative technology areas. The EDF promotes cooperation among European companies and research institutes of different sizes and geographical origin in the EU, strengthening the resiliency and strategic autonomy of Europe.

Among the 61 collaborative defence R&T and R&D projects that were selected and funded with •1.2 billion, Airbus Defence and Space is coordinating the European Defence Operational Collaborative Cloud (EDOCC) project, while Airbus Helicopters is coordinating the EU Next Generation Rotorcraft Technologies Project (ENGRT). The contracts for these projects were signed in December 2022.

EDOCC will create a virtual platform to increase the interoperability, efficiency and resiliency of military operations, which will strengthen collaborative services on the battlefield. The project will study, design and conceptually validate the virtual platform and develop the first version of a services catalogue while identifying appropriate standards and technologies for high performance and interoperability.

ENGRT will focus on analyzing and understanding the needs of European armed forces for rotorcraft operations beyond 2030. The project's partners will study military rotorcraft concept of operations and define key technologies needed for future military rotorcraft. Alternative rotorcraft concepts and architectures will be explored. This project will pave the way for the next generation of military rotorcraft in Europe.

Airbus is also a partner in six further multinational EDF projects and will contribute with its expertise on the following areas of research and development: Collaborative Air Combat Standardisation; Enhanced Cockpit; European Protected Waveform for SatCom; Cyber Threat Intelligence; Advanced Radar Technologies; and Advanced Radio Frequency components.

The European Defence Fund's target is to allocate euros8 billion until 2027.

**GMC**



●● Photo courtesy Airbus



# HENSOLDT and Fraunhofer work together on space surveillance radar • • •

Sensor specialist HENSOLDT has agreed to cooperate with the Fraunhofer Institute for High-Frequency Physics and Radar Technology FHR with the aim of transforming the technology demonstrator GESTRA (German Experimental Space Surveillance and Tracking Radar) into a series-production ready, operationally deployable system called Custodian. To this end, HENSOLDT has acquired the necessary licenses from the Fraunhofer-Gesellschaft and concluded a cooperation agreement.

The prototype was developed by the Fraunhofer Institute for High-Frequency Physics and Radar Technology FHR on behalf of the German Space Agency at the German Aerospace Center (DLR). The radar is currently in operation at the Schmidtenhöhe site training area near Koblenz, where it is providing initial proof of performance. Another component of the DLR contract is, among other things, the commercialization of the technology by a suitable industrial partner. Following a call for tenders in an international competition, Fraunhofer has now awarded the rights for series production to the Ulm-based radar specialist HENSOLDT Sensors GmbH. The two companies signed a corresponding license agreement on January 12, 2023.

"This project is a beacon of German capability, founded on close cooperation between cutting-edge research and a high-tech company. It enables Germany to build an important national capability in the field of a key technology and at the same time make a valuable contribution to international partnerships," said Peter Schlote, member of the HENSOLDT Executive Committee and Head of the Radar Business Unit in Ulm.

"Based on the GESTRA technology, a global network of ground-based radar systems can be established to monitor near-Earth space. The goal is to detect and track space debris, which increasingly poses a threat to space travel and to the deployment and operation of satellites," adds Professor Peter Knott, institute director of Fraunhofer FHR.

The Fraunhofer FHR and HENSOLDT team is eagerly awaiting the announcement of potential customers' intentions to award contracts. Particular attention is being paid to the German Armed Forces: "It is known that the German Bundeswehr is aiming to procure independent sensor technology for space reconnaissance," says Peter Schlote. "Knowing full well that the German Armed Forces have high requirements, the specialists of the Space Command would be our first choice as a partner."

"Bringing cutting-edge technology developed at Fraunhofer FHR into operational use with the Bundeswehr together with industrial partners is one of our inherent tasks," said Professor Knott. "GESTRA plays a special role in this for us, as it is one of the largest development projects in our history in Wachtberg."

HENSOLDT, Fraunhofer FHR and the German Space Agency have established a coordination committee to support the commercialization of the Custodian technology, which also serves as a platform for joint activities to build an international radar network.

A cooperation agreement between HENSOLDT and Fraunhofer FHR ensures that future developments of the technology can also be incorporated into the system as capability enhancements. **GMC**

## In brief

SRC has been awarded a contract by the SOSSEC Inc. Consortium on the SCEC OTA and in conjunction with DEVCOM C5ISR to develop a prototype radar for Active Protection System (APS) application that will address existing capability gaps in currently fielded systems.

The Combat Operations Battlefield Radar (COBRA) development by SRC will provide the US Government with an innovative prototype radar.

"We are proud to work with the US Army to develop another innovative, lifesaving solution to a challenge facing our armed forces today," says Kevin Hair, President and CEO of SRC.



# WALTON DE-ICE

**Antenna De-Ice Systems:**

**HOT AIR**

**Snow Shield**

**Ice Quake**

**Portable Radome**

• 24/7/365 Support & Field Services

• Unmatched Performance & Cost-Efficiency

• Global Leader | 40+ Years

+1 (951) 683-0930

sales@de-ice.com

www.De-Ice.com

Visit us at:

**SATELLITE 2023**

Booth # 2418

March 13-16

# Italian industry signs contract for next development phase of 6th generation air system ●●

The team of Italian companies that will participate in the development of the new Global Combat Air Programme (GCAP) have signed a contract to support the Italian Ministry of Defense in the programme's new concept & assessment phase and related demonstration activities. The team, which comprises Leonardo - as a strategic partner - and Italy's leading companies in their respective domains: Elettronica, Avio Aero and MBDA Italia, will progress technology development in support of the GCAP "system of systems" concept, based on sixth-generation combat air platforms operating in multi-domain scenarios.

Industry will collaborate with universities, research centres, SMEs and start-ups, allowing for the exchange of knowledge and growth of skills at a national level, all in close partnership with the Italian Ministry of Defence. The Ministry will be responsible for defining operational needs and directing technological development, drawing on industry support.

Alessandro Profumo, Chief Executive Officer at Leonardo said: "This new phase is a crucial step in the process of identifying and making available the innovative technologies that will ensure our defence capabilities make the necessary generational, technological and operational leap forward, allowing our national enterprise to reach the highest level of excellence and strategic autonomy. As part of the GCAP programme, Italian companies will play a fundamental role in the future of the defence industry at a national and international level. This will take place in a framework of growth that strengthens the operational capacity of our Armed Forces while at the same time generating positive returns including technological, economic and social progress for the entire national ecosystem."

Enzo Benigni, Chairman and CEO of Elettronica said: "With the launch of this new phase of the GCAP programme, we are developing a plan for technology and industry that will move Italy's technology sector from the Typhoon era, the last major European combat air development programme, into a new era of combat air underpinned by sixth-generation capabilities. The wider geopolitical context underlines how vital it is to achieve the right level of readiness, interoperability and availability of technologies. By doing so, we will be prepared to manage any crises that may affect us. Italian industry's significant role in the GCAP programme will secure a national, European and international legacy, helping to cement the concepts of strategic autonomy and technological sovereignty. Elettronica is ready to contribute and recognises that the objectives that the GCAP programme aims to achieve are also its own."

Riccardo Procacci, CEO of Avio Aero said: "Today's challenging geopolitical context requires technological solutions that focus on operational excellence and the ability to adapt to future scenarios. The GCAP programme is responding to this need and will support the requirements of the Armed Forces while guaranteeing strategic autonomy. Avio Aero, as a European company in the propulsion sector and a long-term partner of the Armed Forces, is bringing its capabilities and recognised technological excellence to the programme as well as continuing to invest in the development of innovative technologies with the support and involvement of its network of collaborations with universities, research centers and SMEs."

Lorenzo Mariani, Executive Group Director Sales and Business Development at MBDA Group and CEO of MBDA Italia, said: "By participating in the GCAP programme and this second phase of our contract, MBDA Italia and our partners at research centres and SMEs will deploy our collective ability to manage the effectors and related technologies required for the system of systems. These technologies will form the basis of complex systems for national air defence. The ability to counter the most challenging threats will be a key element of the performance of a sixth-generation combat air system."

In support of the GCAP programme, Italy has already earmarked 6 billion Euros for investment in research and development that will allow for the launch of technology development projects in areas of strategic interest. These will allow Italy's national industry to participate in the future development phases of the system-of-systems.

The development of a national collaborative work environment, a digital infrastructure underpinned by advanced security, will enable information, services and activities to be shared securely, supporting the subsequent implementation phases via a secure and classified virtual environment. The activation of projects which will deliver technological growth in areas of strategic interest will allow Italy's national industry to play a substantial role in the development of the system of systems. This activity will be vital in achieving an appropriate level of national sovereignty.

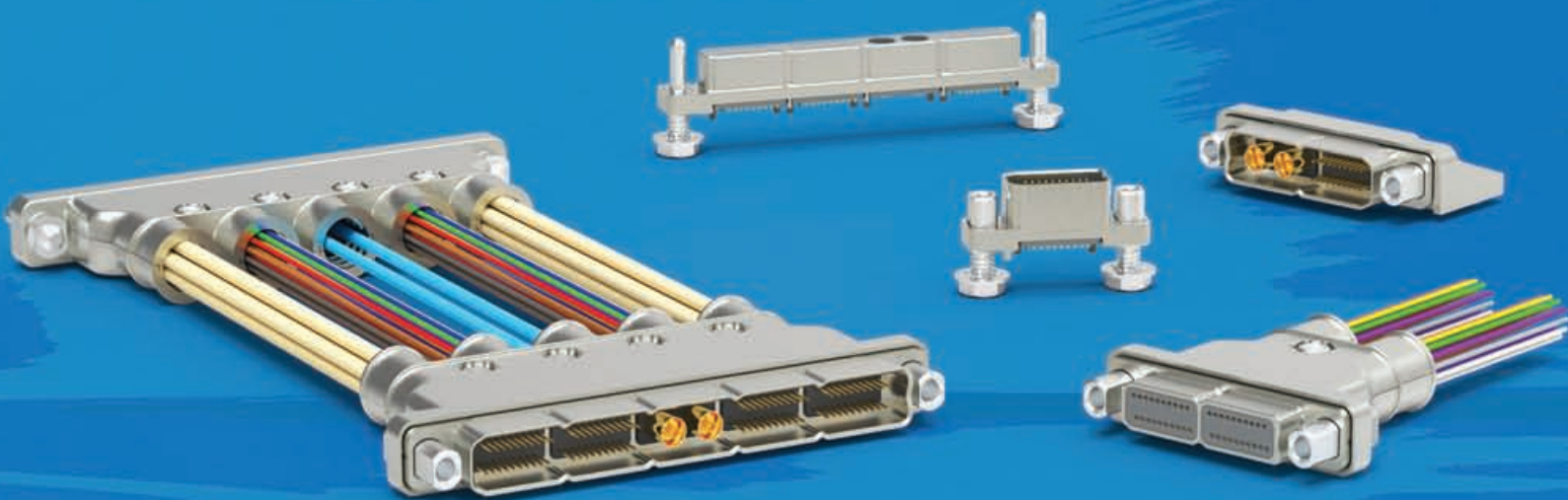
This initiative is also laying the groundwork for further international collaboration in the development of technologies relating to sixth-generation combat air platforms by enhancing Italy's national industrial competitiveness, its strategic autonomy and the academic and professional skills of current and future generations. In support of this goal, companies have already begun to invest in research, to activate collaborations with universities and to support technology incubators in the innovation sector by promoting the most promising ones nationally and internationally.



●● Photo courtesy BAE Systems

GMC





# Introducing SINEERGY®

- Speeds up to 25Gbps
- 4 points-of-contact – withstands a very rough ride
- High-density, configurable in 1-5 bays
- Interchangeable molded signal & SMPM RF insulator bays
- Tested & qualified based on MIL-DTL-83513 performance requirements
- Discrete wire, SMPM RF, & Twinax cable variations

a i r b o r n . c o m



● ● Daniel Gizinski, Comtech's Chief Strategy Officer for Defense, Comtech

# Dedicated cybersecurity development integration needed to defend cyber threats ● ●

With so many disquieting revelations about the power and ubiquity of today's cyber-threats, technology developers, industry partners, and government divisions are becoming increasingly concerned about the strength of today's cybersecurity capabilities. Daniel Gizinski, Comtech's Chief Strategy Officer for Defense, spoke with us about the nature of the threat, and how governments, defense agencies, and the private sector can best respond and prepare for the future.

*Laurence Russell, Associate Editor, Global Military Communications*

**Question: The industry has been fielding an increasing number of conversations around cybersecurity in their communications, especially in mission-critical spheres. How does Comtech react to that discourse?**

**Daniel Gizinski:** Cybersecurity is major area of focus in our industry at large. This is a frontier that continues to make headlines due to the increasing seriousness and frequency of cyber-attacks and the exploitation of security flaws in high-profile proprietary systems.

The rate of today's cyber-attacks has inevitably led to the development of more cyber-hardened solutions across industries and infrastructures. As we understand the progression of cyber-threats, technology developers and other industry partners are working to, future-proof cyber defense capabilities as much as possible. In many cases, cyber solutions and services used by defense markets are fielded over a much longer time horizon, sometimes over 25 years. The way we thought about cybersecurity 25 years ago feels ancient in comparison to the reality in 2023, so we need to ensure our technology fielded today can continuously evolve to remain in step with the increasingly sophisticated nature of the threats we are facing today and the ones we anticipate will appear in the future. In many cases systems will be fielded with zero-day vulnerabilities, and there's a race between the operator and malicious actors to patch or exploit the

# GMC

## Q&A



● ● Comtech's new tech manufacturing facility in Chandler, Arizona. Photo courtesy Comtech





● ● Featuring extremely compact form factors and an extensive list of software options, Comtech's SLM-5650C2 modem can be easily integrated with a wide range of platforms and mobile manpacks

system. It's a bit like Erwin Schrodinger's infamous thought experiment where a cat in a box is simultaneously dead and alive – these systems are both secure and compromised.

**Question: What trends have you noticed prevailing across industry forums and conferences?**

**Daniel Gizinski:** As we begin to deploy multi-constellation, multi-orbit, hybrid networks, there's an exponential increase in network complexity. In a lot of cases, a future user leveraging a converged network may have terrestrial and satellite working together with Troposcatter or microwave all into one network which provides a very resilient capability, but also opens the potential cyber-attack surface of the network, meaning you have a network that's only as strong as its weakest link.

Once an adversary or other infiltrator finds their way into a conventional legacy network through one of many virtual doors, that infiltrator will often enjoy relatively unfettered access to the rest of the network. It's analogous to breaking into an apartment – it doesn't matter if you came in through a door or a window, an intruder would have access to everything inside that isn't secured.

Today, we are moving to a Zero Trust model as a way to prevent these breaches. This zero trust model assumes the perimeter security may be breached at some point, so we need to re-validate access continuously to protect the network.

That's why Comtech's been working with partners across the industry to support Zero Trust network architectures – the principle of least privilege across the board, which limits access dependent on the endpoint being interfaced. A well implemented Zero Trust architecture needs to be lightweight and limit the burden on users, while providing the increased security required to support hybrid networks.

**Question: One of the concerns posed at Global MilSatCom 2022 was the unclear extent of Russia's cyber capability. With the Kremlin being keen to boast of "nuclear level" cyber weaponry, should we take the threat more seriously, or see this posturing as the kind of spurious supposition we've got used to seeing from the Putin administration?**

**Daniel Gizinski:** There are likely elements of truth to both sides

of the coin. Projecting the impression of dominance serves a purpose in conflict, serving as a potential deterrent against escalation. We have grown accustomed to a degree of puffery from this administration, and some of that has likely carried over into this cyber posturing as well. At the same time, the nature of what we're hearing and the evidence we've seen of successful Russian cyber aggression means we must presume these capabilities exist and ensure our defensive cyber architecture and response focus is structured to address sophisticated cyber offensives from adversaries and other malicious actors. We also must be mindful as we develop modern platforms that there is value in maintaining technical sovereignty over as much of the architecture as possible, including domestic manufacturing and engineering. COVID-related shortages in semiconductors and recent fuel shortages in the world bring to the front of mind the risk of reliance on external sources for critical infrastructure and support.

**Question: At the UN Open-Ended Working Group (OEWG), a Russian delegate labelled commercial satellites as "legitimate targets" in their wartime military objectives, owing to their capability to serve forces they oppose. Given that the country proved their anti-satellite missile capability in late 2021, do these words reframe the context with which corporations supply modern war efforts?**

**Daniel Gizinski:** As anti-satellite weaponry has improved to the point where these lines of communication can be cut readily, there's been an increased focus in how a government defends their sovereign satellites. The statement Russia made at the UN open-ended working group was interesting and certainly generated a lot of conversations between satellite operators and governments on indemnification if a commercial satellite were targeted. Most commercial satellite operators are beholden to shareholders, and many of them will take this message as a sign they must proceed with the assumption that their satellites will be a target and may require certain assurances. Conventional technical assets serving IT infrastructure, email systems, and data storage have been targeted for attack during conflicts, and satellite operators have invested in improving their cyber posture as a result.

It is important to note that military users are becoming a significantly small, even fractional, user/subscriber population on our continually expanding, global, hybrid (multi-orbital) commercial satellite network infrastructure. In fact, as military users move toward implementing the ability to roam seamlessly in, and among various commercial satellite networks, military users essentially 'hide in plain sight' due to the fractional nature of the military user profile, relative to the intensely dominant commercial user population utilizing these networks.

This 'fractional user' perspective dramatically increases the complexity of an adversary's decision calculus in terms of targeting commercial satellite networks via kinetic, or non-kinetic means.

The point being, is it reasonable for an adversary to target a commercial satellite network when the adversary cannot be sure that the military user is using that network at all, and if they are, it is on an interim, and fractional basis?

**Question: What is your take on revolutionary emergent tech such as general AI and quantum? With optimists suggesting these technologies could be available in as little as 5-10 years, their presence in warfare could rewrite our understanding of the cyber domain.**

**Daniel Gizinski:** That's certainly true. Both technologies are game-changing, with the potential to cataclysmically impact parts of our industry.

Quantum of course comes up frequently in the context of cryptography, which has motivated a significant spend on quantum-resistant security. We've seen a first tranche of quantum resistant algorithms introduced, and we anticipate continued focus in developing and deploying these techniques. Continued use of legacy encryption schemes potentially opens users up to the data being exposed at some later date, where it may still be sensitive, so there's a real urgency to get these capabilities deployed and operational.

Artificial Intelligence (AI) tends to be discussed as a

homogenous set of questions despite there being many varying levels of AI and machine learning (ML) solutions currently out there and on our horizon. Presently, many systems relying on AI/ML for defense still require a human "in-the-loop" for real decision-making but reducing some of the repetitive tasks reduces the cognitive load on the human operator. With the AI/ML capabilities focused on executing the repetitive tasks, the operator now has room to focus on making the most critical decisions in any given situation. The ability to identify, monitor, and react to threats in a network without human involvement is a true sea change in the cyber domain, and of course, it also allows for automated approaches to respond to a wide range of cyber threats and/or attacks, both in cyber and other domains.

**Question: What are developers missing right now?**

**Daniel Gizinski:** I would say the biggest thing is building a culture of cybersecurity into our organizations across industries and levels of government administrations. Historically, the approach to developing and modernizing cyber has been very rules-based, as with things like the National Institute of Standards and Technology (NIST) risk management framework (RMF) checklists that administrators need to follow and controls they need to implement.

Today, it's more important than ever to ensure that cybersecurity is being delivered as an integrated part of the development process for every piece of technology you're working with, rather than a set of policies layered on top of inflexible software. You need the team building and upscaling your technology to intimately recognize the scale of the challenge in cybersecurity and the future threats they'll need to address down the line.

We need to learn how to live and breathe cyber hygiene as part of daily operations, not write this problem off as a few lines of official policy on paper. Cybersecurity has become an extension of our systems themselves, not something to be bolted on after installation.

**GMC**



Comtech's SLM-5650C2 Software-defined modems are designed to support multiple waveforms and multi-orbit terminals for military and commercial applications, with the flexibility necessary to maintain cyber posture today and into the future



AvL

# **HARSH WEATHER?**

**Communicate through extremes**



**1.6m Manual Point Tri-Band Terminal**  
**Operational winds to 60 mph**  
**MIL-STD-810G tested**  
**MIL-STD-188-164C & Skynet compliant**

Let's talk harsh weather comms @ SATELLITE ♦ Booth 2325



● ● Camellia Chan, CEO and founder of X-PHY, a Flexxon brand

# A digital backbone: how it strengthens and weakens national defence ● ●

Governments are engaged in an arms race against cybercriminals to implement measures which support the construction of a firm digital backbone. Underpinning this strategy is the effectiveness of Zero Trust models at all levels, working in tandem with advancements in AI and ML, and a change in approach about where they're deployed, to combat next-generation cyber challenges from individual and state actors.

*Camellia Chan, CEO and founder of X-PHY, a Flexxon brand*

**For many of us, cybersecurity tends to be viewed** at an individual level. We have antivirus software installed in our computers and frequently hear of people around us falling prey to cyber-attacks. Likewise, organisations use cybersecurity solutions to protect their most critical data, investing in technology and employee training to mitigate the repercussions should they be targeted by cyber criminals.

No different are the risks associated with data protection for national governments – and the geopolitical landscape is as volatile as it has been for decades. The war in Ukraine has placed the world on high alert, but other conflicts across the world are forcing nations to evaluate their defences to ensure they are better prepared for attacks of whatever form. This means defence strategies have in recent years evolved from the physical, to the digital.

## **Malware, DDoS, and the war in Ukraine**

The Russian invasion of Ukraine has been a war on all fronts, with Russian incursions increasingly being supplemented with cyber-sabotage on Ukrainian digital infrastructure. It is a sophisticated and necessarily modern form of military crusade, where the arrival of military forces brings with it a wave of

targeted cyberattacks intended to de-stabilise and threaten the region.

Of all methods, Distributed Denial of Service attacks (DDoS) have been a favourite Russian tactic even before the physical invasion took place. DDoS is a form of cyber-attack in which the perpetrator seeks to make a machine or network resource unavailable to its intended users. These types of attacks present a significant national security risk since they are most effective on high-profile web servers such as banks. In Ukraine, DDoS floods reached an all-time high during the first quarter of 2022, primarily targeting critical infrastructure facilities of Ukrainian enterprises.

But what is the real impact of this military strategy? By using a combination of cyber and missile strikes, the effective transportation of weapons and essential supplies can be heavily affected. According to research by Microsoft, of the roughly 50 Ukrainian organisations targeted by Russian malware since February 2022, 55 percent were critical infrastructure organisations. If anything, this illustrates the importance of a concerted effort by national governments to lay cybersecurity foundations in place.

## **The need to fortify the digital backbone**

Ensuring that your digital infrastructure is bulletproof stands above the factionalism of day-to-day political life. The UK Ministry of Defence's digital strategy is an example of the critical need to consider digital capabilities, and more importantly identify any weaknesses. Among other things, the strategy explores the need for a 'digital backbone' to empower all future abilities in a structured and consistent manner.

In the US, the White House established the Cyber Safety Review Board, a panel of experts charged with examining hacking incidents that threaten US national security. In Singapore, a fourth branch of the military was inaugurated in October 2022. Named the Digital and Intelligence Service (DIS), its role is to combat digital threats on the cyber terrain.

A digital backbone has become an essential arm in the





Photo courtesy X-PHY

maintenance of national stability. It can both empower and weaken a nation's defence if not properly protected. So, as the character of digital competition and conflict has reached new heights, investments into the availability and protection of our most critical data is essential. Part of this involves using a holistic approach, ensuring that there is an equal level of attention to each digital security risk. If we fail to give proper duty of care to cybersecurity standards, for instance, critical investments in other parts of our digital infrastructure will be threatened.

#### Adopting a Zero Trust framework with the support of AI

Of the weaknesses facing individuals, organisations, and governments, the capacity for human error is the most significant. In 2022, World Economic Forum (WEF) research calculated that human error was responsible for 95 percent of cybersecurity issues globally, with individuals and organisations remaining one step behind increasingly sophisticated cyber criminals. So,

to guarantee that you are covering all bases with cybersecurity standards, it would be practical to assume that criminal actors have already gained entry to your systems.

Adopting a Zero Trust framework is necessary, where internal and external users are continuously validated to ensure that suspicious activity can be flagged and acted on in real time. It has been defined by the WEF as a 'data-centric approach that continuously treats everything as an unknown'. For organisations and national governments with highly classified information, Zero Trust should be a non-negotiable arm of a cybersecurity arsenal. When combined with regular and updated training for employees on the risks associated with cyber-attacks, staff (who are vital to the protection of citizens) will be better educated in spotting suspicious activity when it happens.

Understandably, the potential for human error can never be fully eliminated. But with Artificial Intelligence (AI), the technology can spot irregularities and suspicious activity quicker than the human eye. Combined with self-learning capabilities in the form of Machine Learning (ML), AI can defend against many types of attacks.

There is also a strong case for bringing critical data back closer to a system's foundations. The use of cloud comes with many benefits, but it also creates a larger attackable surface for criminals to target. Even with the use of Zero Trust, AI and ML, there are so many variables that the technology will be working overtime to monitor for all types of threat signatures and patterns. With a modus operandi of focusing on a known ledger of threats, software defences struggle to accurately identify new forms of attacks.

As such, adding the defence to the more controllable physical layer allows for the AI to monitor a simple read and write pattern, enabling a far more accurate, reliable, and speedy response to incursions to the data storage level.

#### Lessons for defence at the digital frontier

As the defence sector reframes itself around Industry 4.0, an unprecedented battlefield has opened for cyber criminals. Whether acting at an individual or institutional level, cybersecurity risk continues to evolve and diversify. We are seeing a wave of global initiatives intended to combat this risk in the wake of its application to geopolitical conflicts, but are they enough?

GMC



Photo courtesy Bits And Splits/Shutterstock



● ● Ronald van der Breggan, Chief Commercial Officer at Rivada Space Networks (RSN)

# Linking strong cybersecurity to space with Rivada Space Networks ● ●

Rivada Space Networks' aspirations to produce a new constellation of optically linked high-security LEO satellites has drawn plenty of eyes since its announcement. With a fleet of orbital platforms designed to stand up to the critical requirements of a world increasingly under threat from cyber interference, Ronald van der Breggan, Chief Commercial Officer at Rivada Space Networks (RSN) discusses how they are able to deliver what their competitors cannot.

*Laurence Russell, Associate Editor, Global Military Communications*

**Question: Rivada plans to launch 600 laser-linked Low Earth Orbit (LEO) satellites. What is the advantage of optical connections across a constellation?**

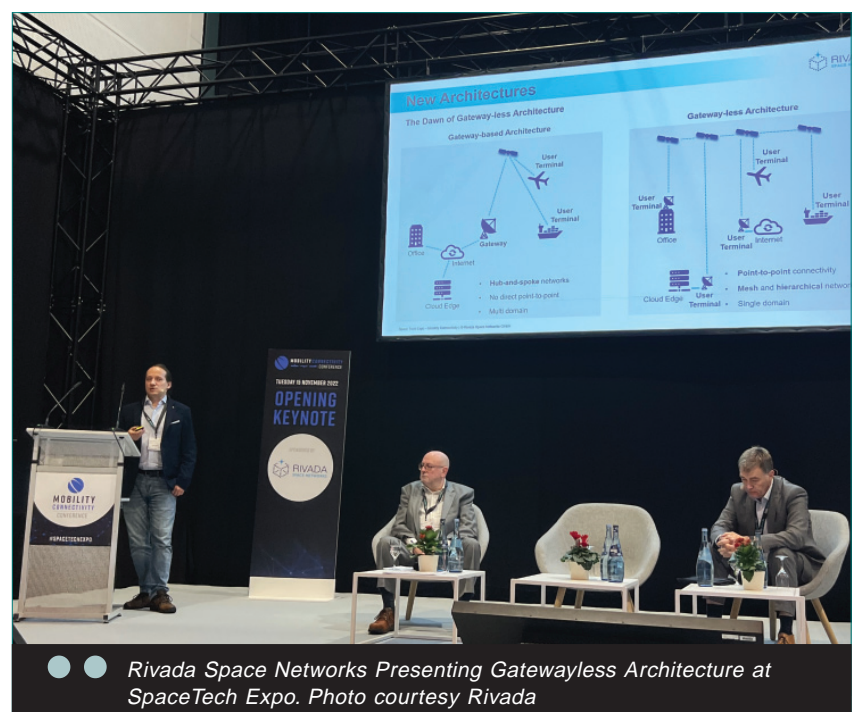
**Ronald van der Breggan:** A conventional satellite constellation without any inter-satellite links (ISLs) or lasers, is basically a swarm of gateway dependent bent-pipe satellites, oblivious to each other's whereabouts and effectively a very expensive access-to-terrestrial network with limited connectivity options. Basically, a gap-filler until terrestrial access networks are available.

Unlike many other existing and planned satellite systems, the Rivada Space Networks architecture will use optical intersatellite links to create a fully connected mesh network in space through which data travels faster than over fiber across the entire globe. By connecting all of its satellites with laser links and running the Multi-Protocol Label Switching (MPLS) network protocol over it, RSN will provide customers with the ability to connect any two points on the globe with low latency and high bandwidth.

The RSN network does not require each satellite in the constellation to be connected to a gateway with terrestrial backhaul to provide end-to-end connectivity. Users can communicate through a single global private network running entirely over the constellation without any terrestrial touchpoint other

# GMC

## Q&A



● ● Rivada Space Networks Presenting Gatewayless Architecture at SpaceTech Expo. Photo courtesy Rivada



# BE PREPARED FOR THE UNEXPECTED

Protect your critical SATCOM applications with  
the unique **CYBER HARDENED IBUCs**.

C-Band | X-Band | Ku-Band | Ka-Band

- ✓ Cryptographic network protocols with SSHv2, HTTPS, & SNMPv3
- ✓ Secret-Key Authentication
- ✓ Multi-Level Access Control
- ✓ Hardened Physical Ports with ASCII
- ✓ Timeline History Logs
- ✓ Enhanced Management & Control

 **SATELLITE 2023**  
MARCH 13-16 | WASHINGTON, DC  
VISIT TERRASAT AT STAND #1529

**Learn more at [Terrasatinc.com](https://Terrasatinc.com)**



than the user terminals or the secure cloud insertion point. This physical separation at the infrastructure level significantly increases cybersecurity and data sovereignty and does so at a global scale.

**Question: Earlier this year at CyberSatGov 2022 US Space Force Col. John Smail explained that space and cyber were uniquely interlinked because satellites were always online and dealing with heavy data loads, making them particularly vital to having assured security in cyberspace. Do you agree with that sentiment?**

**Ronald van der Breggan:** Yes, absolutely. And in fact, satellites which are providing last mile services like those that are not part of an inter-connected space architecture, are indeed an extra 'add-on' vulnerability to the already vulnerable terrestrial systems.

At RSN, we will reduce vulnerability as we keep data in space using satellites in LEO that are designed with security in mind. We can ensure extra secure connectivity and the highest data sovereignty as our space network connects any two points in the world via intersatellite laser links, avoiding terrestrial or non-terrestrial infrastructures or the internet. Furthermore, this makes our network disaster-resilient since it is independent from any other infrastructure.

**Question: In September, Rivada joined the EU Secure Connectivity Programme, working towards assuring uninterrupted, secure, and affordable satellite communications worldwide. How are you contributing to the initiative?**

**Ronald van der Breggan:** The need for secure and resilient global connectivity increases with the digitization of the economy and society and increasing geopolitical and cybersecurity threats. We identified an absolute need to add LEO to this EU multi-orbit constellation approach, with Ka-band delivering the optimal solution in terms of high-throughput networking.

We have submitted our contribution to the Preliminary Market Consultation of the EU Secure Connectivity Programme outlining key attributes of the Rivada Space Network's laser-linked LEO

constellation architecture which includes global reach, ultra-security, resilience and low latency. As a firm believer in common infrastructure platforms for public use, Rivada is also proposing their Open Access Wireless Marketplace platform to optimize the efficient use of the multi-orbit infrastructure capacity amongst the member countries and stakeholders in the project.

Security and Open Access are two of the foundational elements of Rivada's vision of a secure and accessible digital future for all and we therefore aim to leverage the strengths of our satellite communication system in combination with our unique, patented Open Access Wireless Market Platform to enable an efficient use of spectrum and facilitate a fair distribution of capacity to member states. We are proud to be joining the EU's multi-stakeholder Secure Connectivity Programme, mobilizing the space and technology sector to provide an independent and secure communications infrastructure for Europe.

**Question: What is your opinion on onboard processing in satellites. Does working at the edge disaggregate information nodes to widen attack area, or does it position critical functions at a hazardous frontier?**

**Ronald van der Breggan:** With all of the current constellations putting the satellites at the edge of a terrestrial network, providing backhaul services through a gateway, this is indeed a fair question to ask. The RSN constellation however *is* the network. Our satellites are as much core routers as they are access routers, but they are routers! This means we can pick up any traffic right from the source and carry it to its exact destination, for which Onboard Processors (OBPs) are indeed used to perform all the necessary routing and switching on board the spacecraft.

In the case of RSN, the onboard processing positions critical functions in the core, not so much at the edge, and in doing so we significantly reduce the threat surface by offering security on the lowest level of the Open Systems Interconnection (OSI) model, the infrastructure level.

**Question: With many experts more concerned about threats**



● ● Rivada Space Networks - Quantum Encryption. Photo courtesy Rivada Space Networks



**from cyber than any other warfare domain, what should our priorities be for defending satellites from being breached?**

**Ronald van der Breggan:** With the recent events in Ukraine, securing our communications networks is a major concern. Data security and sovereignty are a key priority for Rivada and our network is being designed with a high degree of cybersecurity and with the highest level of security protocols.

Our system can connect any two premises without touching any terrestrial networks. This creates a private network that does not travel through nodes in multiple jurisdictions owned by third party providers, significantly reducing unwanted jurisdiction over, or ability to intercept data traveling over our network.

Unlike many other existing and planned satellite systems, the Rivada network will not require each satellite in the constellation to be connected to a gateway with terrestrial backhaul to provide end-to-end connectivity. This allows users to communicate through a single global private network running entirely over the constellation without any terrestrial touchpoint other than the user terminals or the secure cloud insertion point.

This physical separation at the infrastructure level significantly increases cybersecurity and data sovereignty and does so at a global scale. In addition to the security inherently provided by keeping data in space, we are adding quantum encryption capabilities to our system which will enable us to deploy the most secure communications network in the world.

**Question: In October, you signed an MoU with SpeQtral on the development of quantum encryption solutions. Could you outline that news, and explain the potential of quantum cyber capability?**

**Ronald van der Breggan:** We are very focused on security and SpeQtral is too. It is our ambition to keep data safe, both by offering solutions in space and facilitating quantum encryption for terrestrial infrastructure. With the geopolitical and cybersecurity threats of recent months, the sector is increasingly looking to LEO constellations and a fundamentally different network architecture to provide connectivity that meets today's demands for security, latency, throughput, reach and mobility.

Quantum-secure communications systems and specifically Quantum Key Distribution (QKD) technology are seen as crucial elements in the development of forthcoming highly-secure, satellite-enabled connectivity networks. QKD uses quantum entanglement to distribute encryption keys to secure communications networks. SpeQtral's QKD technology platform enables the creation and distribution of computationally

uncrackable encryption keys, by leveraging the laws of physics instead of computational algorithms.

Rivada Space Networks is partnering with SpeQtral to demonstrate the technical compatibility of adding a QKD encryption layer to enhance the security of communications over LEO satellite constellations. In 2024, RSN will start the launch of its 300-satellite laser-connected constellation with four precursor satellites and SpeQtral will launch its QKD satellite, SpeQtral-1. This will allow RSN and SpeQtral to jointly establish quantum-secure data links over the RSN precursor satellites and validate both the space and ground station terminals required for QKD-enabled encrypted traffic on the Rivada Space Networks constellation.

**Question: What can we expect from Rivada in the years ahead?**

**Ronald van der Breggan:** A highly disruptive and unique network which will provide a fundamental change in the availability of global end-to-end enterprise-grade connectivity. For the first time, a highly secure satellite network with pole-to-pole reach will be available and offer latencies similar to or better than terrestrial fiber.

This network will also leverage the unique strengths of satellite communication, such as the ability to connect platforms on the move, full coverage of the high seas and difficult to connect geographies to open up new opportunities in the telecom, enterprise, maritime, energy and government services markets. RSN's low-latency network will facilitate the fundamental shift from local storage to cloud-based, network-centric operations, meeting the requirement for an enterprise grade "on-demand" experience anywhere in the world from any platform.

Our recent membership of the Global Satellite Operators Association (GSOA) also demonstrates our commitment to working alongside other global satellite operators to drive industry leadership in the face of unparalleled innovation in the space sector, an insatiable demand for all types of connectivity, and a need to bring sustainability to space.

We are also committed to building a strong and resilient communications ecosystem and infrastructure for Europe and having just recently joined the EU's multi-stakeholder Secure Connectivity Programme and the ITU Partner2Connect initiative to further digital transformation, we expect to rapidly move forward with executing Rivada's vision of a secure and accessible digital future for all.

**GMC**



● ● Rivada Space Networks Team. Photo courtesy Rivada Space Networks





● ● Remote site. Photo courtesy Speedcast

# Cybersecurity as a service: Enabling workers to withstand cyberattacks from the most remote of sites ● ●

Cyberattacks have been an ever-increasing threat to all devices across the world, no matter the industry. Check Point Research recently found that the number of cyberattacks in the third quarter of 2022 had risen by 28 percent when compared to the same period the previous year. In the aftermath of the COVID-19 pandemic, there has been a monumental shift to remote working, and this has only compounded the vulnerabilities as new attack vectors are exploited.

*Sandro Delucia, Product Director at Speedcast*

**When it comes to protecting data, most companies** are good at 'locking the front door' – providing adequate cybersecurity defences to prevent any dangers and potential repercussions of a successful cyberattack against their main networks. However, all too often there remain gaps in a network that hackers can exploit.

One area of the industry often overlooked when it comes to cybersecurity are the remote sites found at sea or on land. Employees cannot simply reach out to an onsite cyber-security professional should a cybercriminal target its systems, and therefore must rely on alternative methods to ensure its sensitive data and operations remain secure.

## **An evolving cybersecurity landscape**

Cyberattacks continue to grow both in terms of numbers and

levels of complexity and can be attempted through several different avenues. Hackers often target crucial satellite communications, compromise email systems, and find access to systems that any unsupported software uses in devices across a network. Illicit tampering with the update processes of third-party systems onboard a vessel or site can also provide a gateway for a potential attack. Shipping and maritime operations often fall victim to such threats in part due to the value of the cargo onboard, but also due to their position within an overall supply chain. Unsecured remote sites can also provide the key for hackers to unlock an organization's entire network.

A report from CodeSubmit in 2022 found that remote work has increased by 44 percent in the last 5 years. With most companies seeing a shift towards remote working as a result of the COVID-19 pandemic, this number is only going to rise further. Yet all too often, the domestic devices and protocols found in home networks are not as stringent as the ones deployed in corporate offices, and hackers are utilizing these as a 'back door' into the overall business network and remote site systems. This can become a significant problem for land and sea operations where it can be impossible to reach out to an IT specialist onsite, especially if a system has already been critically compromised.

In December 2021, German maritime operator Hellman Worldwide Logistics reported they were the victims of a phishing attack which crippled its operations for several days. The firm was forced to disconnect its data centers and many of its systems in order to counteract the threat. This effectively cut off the hackers but not before sensitive data was extracted from its



systems, leading to a disruption of its business continuity plans and a significant loss of revenue. Other attacks seen in the maritime industry include those designed to prevent users accessing data unless a ransom is paid, creating severe financial and reputational repercussions for those affected.

A network breach can quickly shut down an operation, causing millions in lost revenue and millions more to repair. Should a remote site be compromised, hackers can reach the heart of the overall network, providing a gold mine of personal and sensitive data to exploit and steal. With IBM Research calculating the average cost of a data breach incident in 2022 as US\$4.35 million, unprotected remote sites should be considered huge security risks. Indeed, significant fines are often imposed on organizations who fail to detect or adequately respond to an attack.

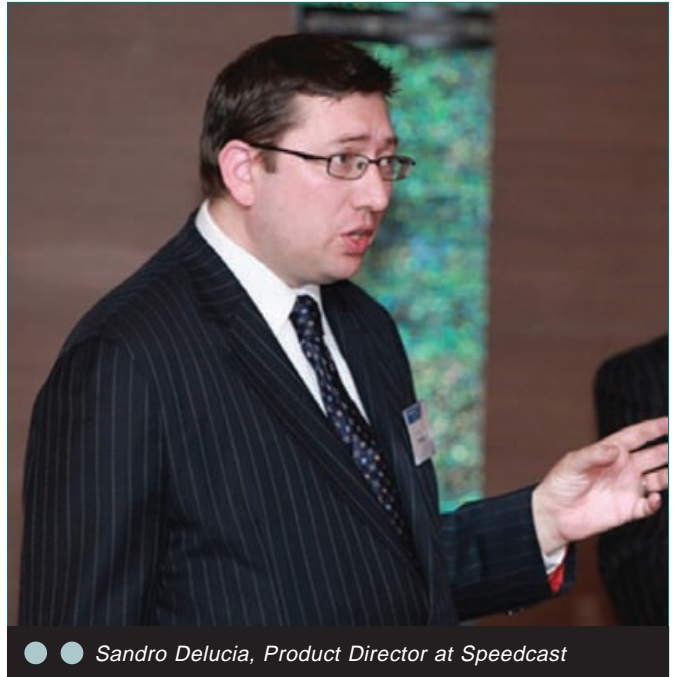
### Overcoming the growing threats

It has become increasingly imperative that – in line with current regulations and the need for seamless business continuity – a leading-edge cybersecurity solution should be deployed to ensure the security of remote sites. This can help to provide vital insight into the very latest threats seen throughout a number of industries and establish an advanced system to overcome these.

This is not as easy as it sounds. The procurement of such technology is often a difficult and costly venture. Managing multiple physical units within a configuration can also be a complex process. One solution to these issues is to leverage technology which incorporates “cybersecurity as a service” as a function. To this end, solution providers are developing smart network management platforms, such as Speedcast’s SIGMA, that provision an industry-standard, next-generation firewall that is maintained through a Virtual Machine (VM). This helps establish a strong security base while carrying out its primary function of providing reliable connectivity to the user.

Operators who look to implement these solutions can utilize the Windows Active Directory, which can be installed as a VM and operate in conjunction with the firewall and relevant security policies to give total control over what users have access to with sufficient granularity. Doing so can provide greater oversight across all networks, enabling the prevention of malicious software over four million times per minute, and providing a strong line of defence against any attack.

Artificial Intelligence (AI) remains the vital cog to handling the sheer amount of threats that systems face daily. AI and Machine Learning (ML) systems provide the tools to *detect*, *alert*



● ● Sandro Delucia, Product Director at Speedcast

and *prevent* any potential attacks on a system and, when combined with a number of threat researchers, threat intelligence against any detected malware can be shared with other organizations in real-time. These concepts are intrinsic to technologies implementing “cybersecurity as a service” within any technology’s capabilities.

### Ensuring the security of your systems

While no single solution can provide an all-encompassing defence against cyberattacks, seamless, end-to-end protection can be implemented for remote sites so long as best-of-breed security technology is leveraged. Adopting technologies that include “cybersecurity as a service” can help protect an operator’s assets, providing scalable and adaptable services to meet the challenges of an ever-changing threat landscape in a seamless manner.

Technologies such as SIGMA which combine the best of content filtering and lightweight synchronization designed specifically for remote sites alongside monitoring and reporting consoles can ensure a site can operate safely and securely, no matter the location.

**GMC**



● ● Photo courtesy Speedcast



● ● Simon West, Cyber Advisory Lead for Resilience

# We're all on the cyber frontline now ● ●

In the wake of a wave of high-profile cyberattacks on commercial business and national infrastructure across the western world, scrutiny has fallen upon the more mundane spheres of civilian enterprise and critical services to strengthen their cyber presence. Simon West, Cyber Advisory Lead for Resilience explains where the flaws lie, and what businesses can do about them.

*Laurence Russell, Associate Editor, Global Military Communications*

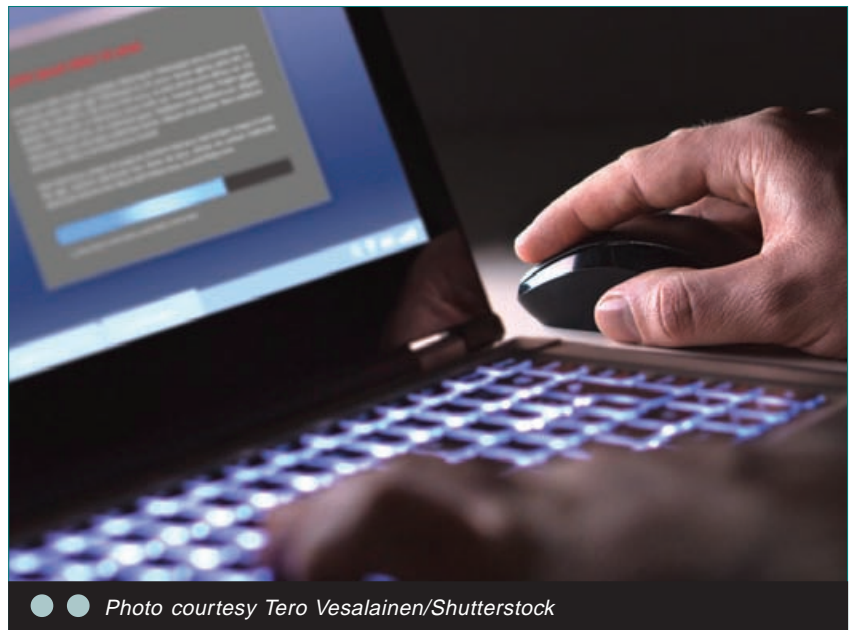
**Question: In September, the Lapsus\$ hacking group claimed responsibility for hacking Uber's network and compromising the Virtual Private Network (VPN) credentials of an external contractor. It's not the first we've seen, for Uber alone, and won't be the last. How difficult are these sorts of breaches to orchestrate for hackers?**

**Simon West:** In terms of orchestration, it's certainly easier now than it has ever been. Especially with the likes of groups such as EvilProxy. Since late September 2022, there has been a significant increase in the number of Business Email Compromise (BEC) cases ending in attempted payment fraud. Most of the cases appear to be linked to a global phishing campaign using a new tool called EvilProxy. This began to be offered as a service on the dark web in September 2022 and allows threat actors to bypass some forms of Multifactor Authentication (MFA) to compromise user accounts.

**Question: Lapsus\$ bypassed Uber's multi-factor security with a push request. Does this reveal more about the fragility of conventional systems and multi-factor than it appears?**

**Simon West:** There is a risk that organizations will fall victim to this new BEC attack method if existing defences are not fine-tuned:

- EvilProxy bypasses some forms of MFA, which many organizations rely on as their primary defence against account compromise.
- Current campaigns are using previously compromised accounts to send out further phishing emails, which means recipients are receiving convincing phishing emails from people they trust.
- Phishing landing pages are more convincing than ever, often being specifically tailored to the victim and not generic in nature.
- Certain industries and sectors are being heavily targeted – legal, insurance, real estate, and financial services. It's only a matter of time before all sectors are under threat.



● ● Photo courtesy Tero Vesalainen/Shutterstock

# GMC

## Q&A



The best ways to defend against EvilProxy attacks are:

- Using hardware token MFA methods (FIDO2 security keys).
- Configuring Microsoft Intune compliance to deny access to untrusted devices (or configuring such a policy in an equivalent mobile device management platform).
- Password-less authentication methods such as Windows Hello for Business because it is more secure than using a password since it uses biometric authentication – you sign in with your face, iris, or fingerprint (or a PIN).
- Limiting connectivity to trusted IP ranges and geographic locations with the caveat that geo-blocking of IPs can be easy to bypass by threat actors using VPN services and may not be appropriate for a globally dispersed workforce.

While one of the most reliable protective methods, trusted device policies can represent a complex and extensive undertaking, which large organizations with thousands of legitimate endpoints may struggle to implement in a short timeframe.

**Question: Hostile states have been keen to hint at overwhelming cyber capability that they have yet to deploy. Given what we've already seen, do you have any anticipation of a world-changing cyberattack in the next decade? A digital 9/11?**

**Simon West:** There is no question that the nation-state capability is there. The question is what the intent looks like to create such a scenario that ultimately escalates to full-on global kinetic warfare. There are no winners in this type of scenario. Uncertainty in the world is exacerbated by the escalating geopolitical situations in countries like Iran, China, Ukraine, and Russia, to name a few, along with destabilized social systems in politics, policing, healthcare, and education.

The one thing we can be certain of during these times is the ever-evolving cyber threat landscape. Witness the constant introduction of new technology devices, tools, and many other things connected to the internet. Cyber risk and the ability of businesses to be cyber resilient becomes an ongoing challenge as the attack surface increases. So too does the possibility of introducing or being exposed to vulnerabilities within our systems.

This challenge is becoming ever more apparent in the protection and bolstering of our Container Network Interface (CNI). "A major cyberattack on the United Kingdom is a matter of when, not if," says the Head of the British National Cyber Security Centre, Ciaran Martin.

The attacks which affected Ukraine's energy grid in 2015 and 2016 and the 2017 WannaCry attack, which affected the National Health System (NHS), showed us that cyber-attacks need not target CNI deliberately to have significant consequences. More recently it was reported that US-based internet provider Viasat was targeted an hour before Russian operations were launched. This incident on the 24<sup>th</sup> February caused outages for several thousand Ukrainian customers, and impacted wind farms and internet users in central Europe.

Collateral damage is a significant cyber risk due to its systemic nature. Whether intentional or not, organizations involved in the production and supply of energy are increasingly becoming a target for threat actors, especially as these facilities migrate their systems from analogue to digital into the cloud. The energy sector and its sub-sectors remain a top target for nation-state actors due to the potential far-reaching damage an attack on an energy facility could cause. The objective must therefore be to make it as difficult and as costly as possible to succeed in attacking critical national infrastructure—and to continue raising the bar as new threats emerge.

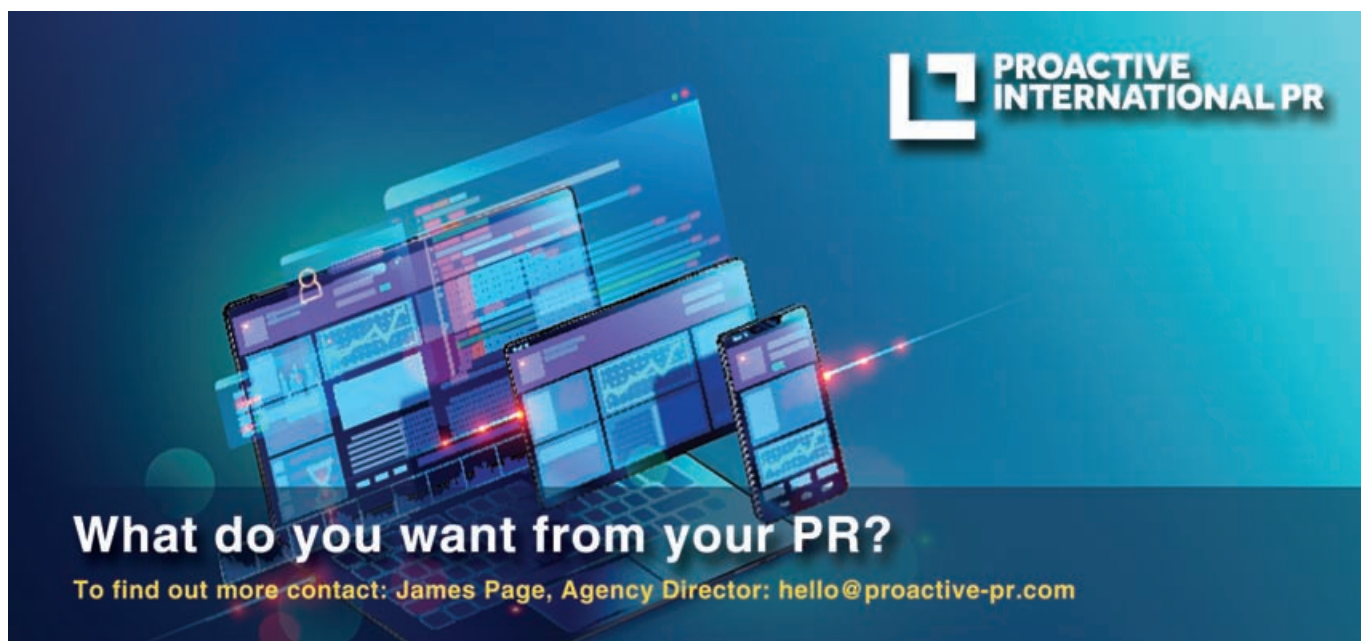
**Question: Infrastructure and enterprise have become very popular targets for cyberwarfare, thanks to their stereotypically lesser cybersecurity standards compared to defence and government assets. What's your advice to them?**

**Simon West:** The UK's critical infrastructure is defined by its government as "Those critical elements of infrastructure (systems, sites, property, information, people, networks and processes), the loss or compromise of which would result in a major detrimental impact on the availability, delivery or integrity of essential services, leading to severe economic or social consequences or loss of life."

Any of these essential services being interrupted might seriously disrupt our lives and the systems they rely on. As our CNI becomes more digital, there are substantial benefits, but also increased cyber security dangers. These services are vulnerable to espionage, targeted attacks from bad actors – including hostile governments and criminals, unintentional data loss, and other cyber threats.

Regardless of the goal or level of complexity of a cyberattack, the public has a limited appreciation of what could befall us as a result. Businesses should be looking at how they can reduce their exposure by incorporating a combination of risk transfer (cyber insurance) and risk mitigation strategies (cyber hygiene).

There are some initial basic steps an organization can take to become cyber resilient:



**PROACTIVE INTERNATIONAL PR**

**What do you want from your PR?**

To find out more contact: James Page, Agency Director: [hello@proactive-pr.com](mailto:hello@proactive-pr.com)

- Have a plan! Having an Incident response plan improves the chances of an effective and timely response.
- Patching - ensure you are up to date with software and OS system updates to remove any potential vulnerabilities.
- Backups and recovery – Ensure you have a strong backup strategy that provides redundancy and the ability to recover within a reasonable time frame.
- Multi-Factor Authentication (MFA) adds a layer of protection to the sign-in process as a core part of Identity and Access Management (IAM).
- Principle of Least Privilege (PoLP) - refers to an information security concept in which a user is given the minimum levels of access – or permissions – needed to perform his/her job functions.
- Training and awareness programme – ensure you cover phishing and then test your employees using phishing simulation tools.
- Establish email authentication protocols to enhance security and reduce fraudulent emails.
- Monitoring – have some form of EDR Network visibility and security.



● ● Photo courtesy Sergey Nivens/Shutterstock

**Question: Kremlin-sponsored hackers have performed infrastructure attacks in recent years, leading to intelligence agencies and defence technology executives seeing the issue as increasingly severe. With responsibility so hard to determine, is civilian cyber vulnerability becoming a true national defence issue?**

**Simon West:** Cyber defence is everyone's responsibility. It is no longer considered to be an IT or security risk alone, but it should be addressed as a business risk. At Resilience, we run cyber incident tabletop exercises for our insureds. We ensure every function within the organization is on the table so we can identify security gaps before incidents happen.

However, the way companies are currently managing cyber risk is still inadequate – its either done in silos of security or insurance, driven by marketing revolving around fear, uncertainty, and doubt, or simply by applying status quo benchmarks from peers that aren't necessarily relevant since everyone has their own risk profile.

As a result, risk managers are overwhelmed and need a guide to the increasing technical complexity. CISOs are fighting tactical fires and need to become strategic partners, and CFOs have a know/do gap and need confidence in a unified approach.

**Question: Marketers and optimistic experts have been telling us for years that everything will be connected and digital very soon, but what we've been missing in that sentiment is that the cyber frontier is now right at the door of civilians and the systems they rely upon. Is that a concept the public is ready for, or would the terrifying truth do more harm than good?**

**Simon West:** The world of Internet of Things (IoT) is already upon us and it's not going anywhere. We could say the smartphone was the original smart device but if we look around our homes today, we are surrounded by smart TVs, kitchen utilities, smart meters, CCTV, even children's toys.

We see cities like Barcelona leading the way as a smart city benefiting from savings and profits made in smart parking, street lighting, and water sprinklers. It's important as a business we understand how these devices encroach into our business operations and what is required to secure them.

We believe companies must now integrate their technology, economics, and behaviour to work together to reduce their cyber risk. We believe that companies can't just be cyber covered or cyber secure, they need to be cyber resilient. This has become a requirement for success.

That is why we exist, and in fact, why we named our company Resilience – to empower a whole new generation of cyber resilient companies.

**Question: What are conventional cybersecurity developers missing in this fight? What working or promising cyber defence strategies haven't been made mainstream?**

**Simon West:** It's easy to fall into the trap of looking for the next best technology when most of the answers you're looking for are right in front of you. There is no point in reinventing the wheel and constantly being on the chase for the next best thing when it could potentially leave businesses vulnerable. The majority of companies need to get the basics right first.

We still see a lot of businesses today primarily focused on prevention, when ideally they should be moving to a posture that includes a proportionate amount of monitoring and response capabilities.

At Resilience, we can help provide this through our proprietary scanning technology which enables us to map our clients' risk profiles and provide them with vulnerability and threat intelligence notifications, thus allowing them to have continuous monitoring so that they can respond to timely actionable information as well as transfer some of their residual risk within their insurance policy.

As a result, they can take a digital hit without having it impact their material ability to deliver value.

**GMC**





# SPACE SYMPOSIUM

S P A C E F O U N D A T I O N

**April 17 – 20, 2023**

Colorado Springs, CO, USA



**JOIN US IN OUR SPACE OR YOUR SPACE**  
In-person or Virtual registrations available

**[www.spacesymposium.org](http://www.spacesymposium.org)**



Register  
now



# New horizons for the defence industry means the outlook is bright for 2023 ●●

Tech-led developments are ensuring that the outlook for the defence industry is positive for the year ahead. Additive manufacturing and more digitized ship manufacturing are just a handful of new approaches set to improve manufacturing processes and military equipment readiness. The ocean is now being infiltrated by uncrewed military vessels and military frameworks are being drawn for space operations – the next frontier of the defence sector.

*Matt Medley, Industry Director, A&D Manufacturing, IFS*

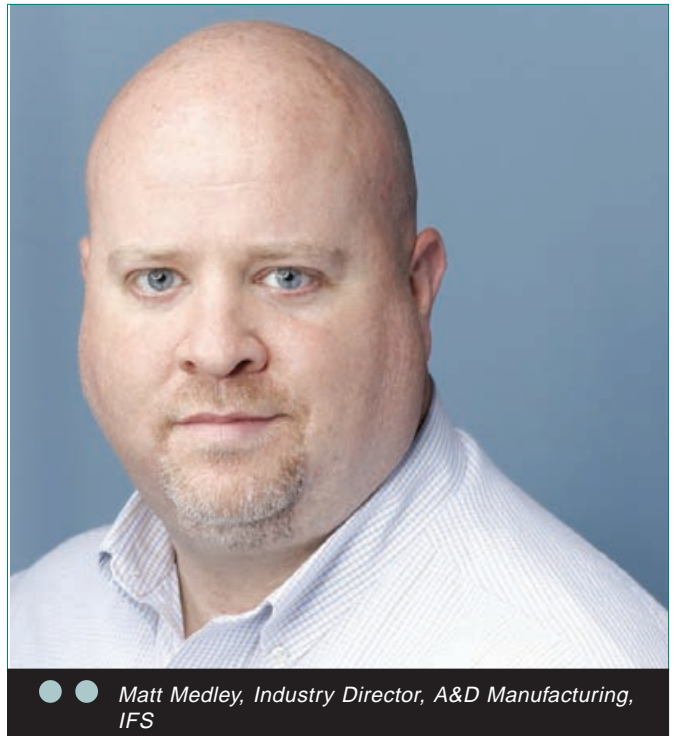
**The outlook for the defence sector is positive in 2023**, despite having to face some macro-level geopolitical and economic headwinds.

Advanced technologies are already being incorporated into operations by leading defence forces, defence contractors, and Aerospace & Defence (A&D) manufacturers. These will ensure they stay one step ahead of hostile forces, remove more war fighters from risk of danger, while exploiting the use of new technologies to minimize the military logistics footprint.

This growth is confirmed in the Deloitte 2023 Aerospace & Defence industry outlook which shows nearly 90 percent of senior industry executives think the overall business outlook for the A&D industry in 2023 is “somewhat to very positive.” Within this report Deloitte also highlights that the driving forces behind this outlook “include growth in new technologies and segments such as AAM, evolving business models in areas such as space, and the use of digital thread and smart factories. All these factors should help the industry grow and create new markets in the coming year.”



●● Autonomous ships. Photo courtesy IFS



So, with these developments powering the A&D industry in 2023, let's look at five areas I see the most potential for growth in 2023 and the future.

## **Prediction 1: The adoption of 3D printing continues – from bolts to bunkers – as half of A&D manufacturers incorporate it to reduce logistics footprint**

The use of 3D printing has increased drastically recently to help military forces repair vehicles, vessels, and aircrafts more quickly. Advancements in that arena have also made it possible for medical resources and safety apparatus to be designed and prototyped for use in the field. Now, the US military are taking 3D printing to the next level with the design of the world's largest 3D printer which is able to print metal parts that are 30 feet long, 20 feet wide and 12 feet high. This makes it a vital part in the progression of military forces using 3D printing for constructing bunkers and runways. The defence industry's use of 3D printing is not expected to slow down—75 percent of industry leaders see 3D printing as being a base protocol in the next ten years.

3D printers can allow for replacement parts to be printed when they are required, compared to the traditional method of waiting for parts from external suppliers which can take up to 25 days—crucial time when hostile forces may aim to target supply lines. This allows for military forces to be more self-sufficient and reduce maintenance wait time. In the long run this will lead to the logistics footprint being reduced for forward operating bases, resulting in forces being deployed more flexibly in rural bases with minimized need for access to extensive supply lines.

Additive manufacturing can bring logistical challenges dependent on where parts come from due to the merging of two normally separate fulfilment approaches, one through a third-party supply network and the other through internal additive manufacturing. This sometimes results in competing Total Asset Readiness expectations due to the number of potential parts the machine can create. However, Machine Learning (ML) and Artificial Intelligence (AI) can be used to augment decision making from traditional logistics personnel and establish the best fulfilment path.

## **Prediction 2: Maritime 4.0 and digital shipyard set to achieve a 19 percent Compound Annual Growth Rate (CAGR) until**



### 2023 – aided by Industry 4.0 technologies

Industry 4.0 has accelerated the manufacturing sector into change with new technology and has now moved on to A&D manufacturing sectors for example, shipbuilding. Maritime 4.0 is beginning to show benefits in terms of improved efficiency when designing, manufacturing, and constructing ships with better coordination, clearer operations, and maintenance. Despite only being in the adoption stage of its journey, the digital shipyard market is expected to experience rapid growth with the market already being valued at \$693 million in 2022 and expected to grow to \$3,967 million by 2030 at a CAGR of 19 percent.

To help with the design and construction of ships, three technologies – artificial intelligence (AI), machine learning (ML), and digital twins – are propelling the development of digital shipyards and Maritime 4.0. According to global professional services firm Lloyd's Register, "The shipbuilding value chain may be empowered to make better decisions and deliver smarter assets by sharing and integrating data from the influx of new AI and ML based technologies that are now becoming evident in both shipbuilding and operational sectors."

The UK Department for Transport recently invested £206 million to support the net zero aims for emissions within the maritime industry. These Maritime 4.0 technologies will allow for a green maritime future reducing CO<sub>2</sub> pollution and emissions from shipyards, but will need the support of cutting-edge software. It will also need to match its expected growth. The construction of such large assets in increasingly digital shipyards requires an industry-specific and enterprise-breadth software system which can manage such a unique construction process.

### Prediction 3: A third of total fleet set to be autonomous vessels in the next 20 years –with continual increase in operational capabilities and deployment

The UK Royal Navy recently gained a game changing Testbed ship with a large surface area for launching UAVs and AUVs which will be tested by NavyX. With a reduced need for room for personnel, there is area for an operation centre and a meeting room aboard the ship. Importantly the Testbed Ship will allow



● ● Photo courtesy IFS

the Royal Navy to deploy the MAST-13 AUV, a water-borne drone capable of identifying mines and gathering information on hostile ships. Meanwhile in parallel developments, the US Navy is unveiling its third unmanned surface vessel 'The Mariner.' The ship is fitted with a government-furnished command and control system, a virtualized Aegis Combat System, and an autonomous navigation system. After a few more upgrades there is hope that 'The Mariner' will begin deployment in 2023. Going forward, the US Navy Navigation Plan (NAVPLAN) to modernize its fleet includes a desired force level of 523 ships by 2024, including 150 unmanned surface and subsurface vessels—making up nearly a third of the fleet.

Autonomous ships will reduce the number of war fighters sailing into danger when out on missions as they allow for ships to enter areas that were previously seen as too dangerous or inaccessible for manned ships, to gain key intel. No longer having



● ● Additive manufacturing. Photo courtesy IFS

the requirement to house personnel means bigger payload capacity, including more fuel, allowing for longer deployments or more sensors for advanced surveillance.

Maintenance controls must be amplified to ensure full mission capabilities and Total Asset Readiness for autonomous vessels as lack of crew has implications for maintenance and sustainment. There is increased criticality of proper ship autonomous self-monitoring across systems, and failure projections will need to be embedded within the design to predict and plan for downtime. Without manned inspections, on-board self-diagnostics and monitoring systems must connect to the broader digital twin ecosystem, a level of automation that cannot be met by yesterday's systems and processes.

**Prediction 4: The new space race – reliance on space for defence and defence opens up huge growth market with CAGR of over 10 percent**

Space is becoming a new operational domain, and the market is expected to take off over the next couple of years growing from \$14.21 billion in 2022 to \$31.90 billion by 2029 at a CAGR of 12.25 percent. It is currently being used to navigate and track forces to avoid detection when delivering supplies or allow for precise strikes on hostile bases, and to improve communication and detect potential threats. The race is on to get ahead in a more militarized space domain—and intergovernmental organizations such as NATO are getting priorities in order as military forces gear up for increasing reliance on space-driven operations. In 2022 this led to NATO publishing an “Overarching Space Policy”, to set out the fundamental aspects of the space domain and its importance in preserving the alliance's security and prosperity.

It confirms that, as part of its policy, NATO will address space as a coordinator between members with space-based assets. It also identifies some key functional areas of focus for the need for space systems such as: space situational awareness, intelligence, surveillance, and reconnaissance (ISR), space-based monitoring of Earth-based domains, satellite communications, position, navigation, timing, and shared early-warning assets. Expect increased focus on the space domain

in 2023 and beyond, as more organizations become part of a growing military ecosystem.

**Prediction 5: Over half of businesses will find themselves in a data breach – underlining the criticality of cybersecurity when deploying new technologies.**

Cyber-attacks are a greater possibility for a defence industry with increased reliance on digital technologies to manufacture, operate and maintain military equipment. Increased cyber risk also comes with autonomous vessels, new digital manufacturing standards, and new operating environments. So, core software is essential to assure all assets and processes are protected. Detection, reporting and solutions to security problems are key software requirements to keep all systems functioning and secure in the event of a potential cyber-attack.

Deloitte highlights the importance of cyber security as a prevalent industry theme in its 2023 Aerospace & Defence industry outlook: “Most A&D companies are expected to also focus on creating visibility deep into their supply chains to improve supply control and coordination and to better manage third-party risk. Industry players will likely reinforce the need for cybersecurity, cloud privacy, and the resilience of the systems and automation to be prepared effectively for any risks within core operations and with key suppliers.”

The increased use of cyber warfare means cybersecurity is now a key requirement of any software infrastructure used within the military supply chain. Pen-tested and secure systems are a must for businesses to avert and respond to threats posed by the increase in cyber risk.

Security focused approach doesn't waver, but we can expect processes, equipment, and deployment models to change

Advancements in four promising areas spanning new manufacturing principles, equipment, and operational models set to help defence forces, A&D manufacturers, and defence contractors.

Despite these advancements a strong and secure digital backbone will be required, to make sure hostile forces can't breach data as the defence sector increases its reliance on digital in 2023.

**GMC**



● ● Photo courtesy IFS



# GLOBAL CONTENT DISTRIBUTION



# STN

## End to End Solutions

SATELLITE  
& IP

PLAYOUT  
& CLOUD

STREAMING  
& OTT

OCCASIONAL  
USE

CO-LOCATION  
SERVICES



WWW.STN.EU



SALES@STN.EU



+386 1 527 2440





INSTALLING  
RELIABILITY

# SKYWAN – THE NEW DIMENSION IN AIRBORNE SATELLITE COMMUNICATION

[www.ndsatcom.com](http://www.ndsatcom.com)

© AIRBUS HELICOPTERS, BART ROSSELLE

 **SATELLITE** 2023®

**ND SATCOM BOOTH #1122**



[www.ndsatcom.com](http://www.ndsatcom.com)