

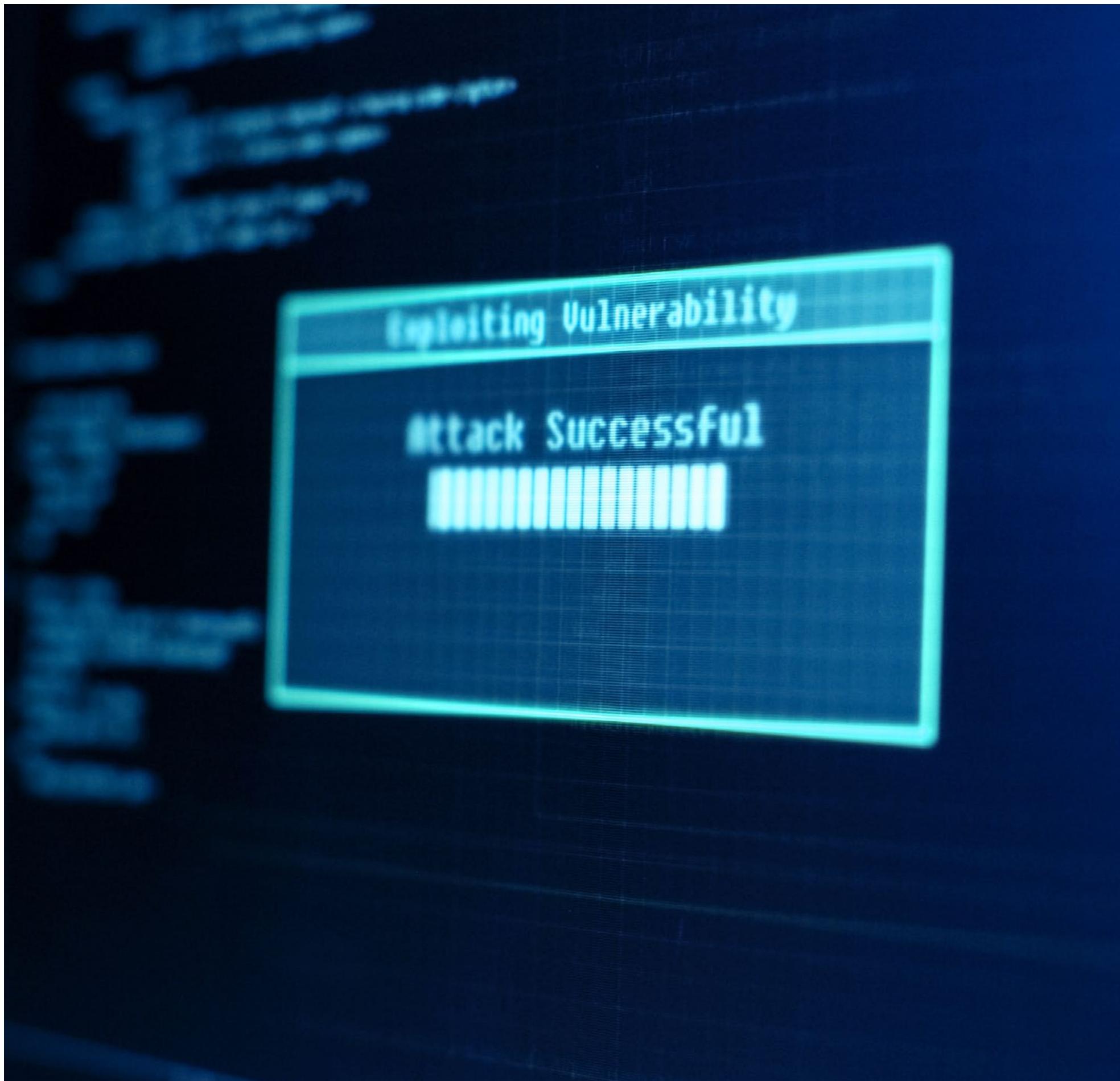
Digital Horizons

A series of reports exploring CEE's digital future

Digital Defence

February 2024

New ways to wage war



For nearly two years, the haunting presence of war has dominated news headlines, with Russia's invasion of Ukraine and the ongoing conflict in Gaza taking centre stage in news bulletins.

Many less high-profile hostilities are also raging. Sipri, the Stockholm International Peace Research Institute, recorded 56 countries experiencing armed conflict in 2022. The UN has warned that the world is facing the highest number of violent conflicts since the Second World War and that 2 billion people — a quarter of humanity — live in places affected by such conflict.

But what is less often mentioned is that the nature of warfare itself is changing, with unprecedented speed.

NATO's view is that there are now five 'domains' of warfare: Land, Maritime, Air, Cyber and Space. Wars have been fought on land and sea for millennia, but war in the air is just over a century old. And we are only beginning to understand what cyber war and space war may mean for the world.

Digital technology is fundamental to this transformation. While cyber is naturally digital, digital developments also underpin innovation in each of the four domains.

NATO's vision of the future includes the connection of command functions across all five domains through a common network, with a 5G-like network linking mobile command posts and handheld devices, as well as bringing advanced data analytics, cloud computing and AI onto the battlefield.

Learning lessons

The war in Ukraine has highlighted many ways in which digital technology is changing conflicts, from the ubiquity of drones to the presence of mobile phones on the battlefield and the analysis of unprecedented levels of data from diverse sources. It is also the first major kinetic conflict to feature extensive cyber attacks. So it is no surprise that governments across CEE – and elsewhere – have been seeking to learn lessons from Ukraine for their own defence.

One such lesson is that the private sector is now key to innovative and integrated warfare. While Ukraine has received much aid from friendly governments, it has also relied on support from a wide variety of tech and defence companies, both large and small. Armed forces looking to develop their own cutting-edge systems know they are more likely to find the specialist expertise and capacity they need in businesses than in government departments.

Not all such businesses are defence businesses. Many companies active in the digital arena will have some intellectual property or products that are also capable of 'dual-use' application or conversion to defence use.

Even more importantly, thanks to the spread of networked devices, all businesses are potentially vulnerable to attacks aimed at creating social or economic disruption. So it is also vital that companies – especially key companies in critical sectors – are well-placed to resist and recover from cyber attacks.

A massive market

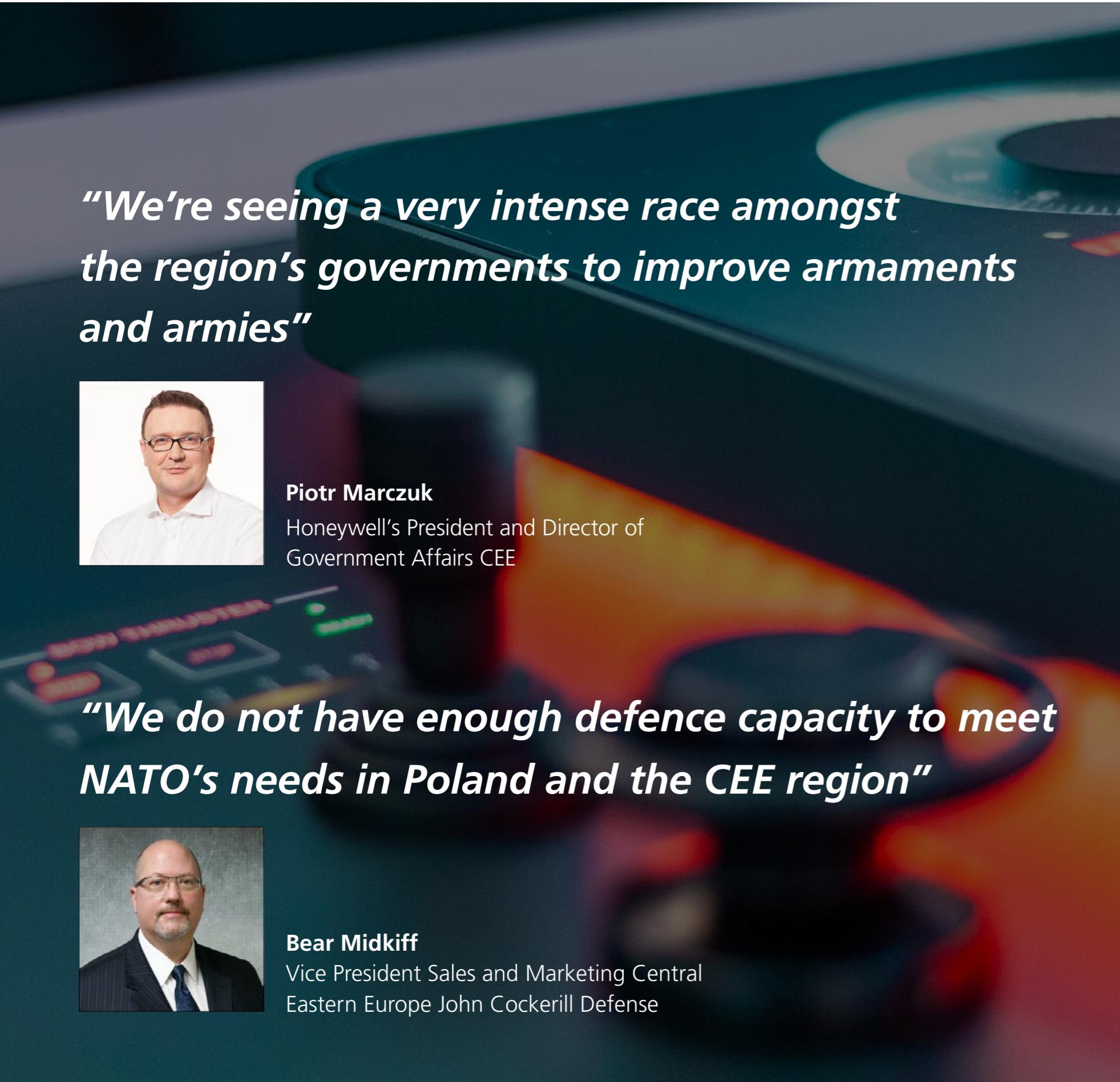
Global military expenditure in 2022 was a record \$2.2 trillion, according to Sipri, with spending in Europe rising at its fastest rate for at least 30 years. Growth will certainly continue in the foreseeable future.

There will be even faster growth in cyber security technology and services. In 2022 McKinsey estimated the total addressable market for this to be about ten times larger than the \$150 billion that was spent on it in 2021. As the frequency and severity of cyber attacks increase, both public and private sector organisations, including those which have not previously regarded themselves as prime targets, will be budgeting much more to defend themselves.

As security challenges grow ever more complex, multidimensional and fluid, heightened expenditure on defence – both real-world and cyber – becomes a necessity, not a choice. The rest of this paper looks at some of the issues around that expenditure, and the opportunities and challenges that exist for businesses seeking to meet these defensive needs.



A wake-up call



"We're seeing a very intense race amongst the region's governments to improve armaments and armies"



Piotr Marczuk
Honeywell's President and Director of Government Affairs CEE

"We do not have enough defence capacity to meet NATO's needs in Poland and the CEE region"



Bear Midkiff
Vice President Sales and Marketing Central Eastern Europe John Cockerill Defense

Russia's invasion of Ukraine has been a wake-up call for many nations, with CEE governments quick to respond. Countries bordering Russian territory saw some of the biggest increases in defence spending in 2022, with Finland's up 36%, Lithuania's 27% and Poland's 11%.

"We do not have enough defence capacity to meet NATO's needs in Poland and the CEE region," says Bear Midkiff, Vice President Sales and Marketing Central Eastern Europe John Cockerill Defense.

"The peace dividend we were so anxious to enjoy, and the umbrella of safety felt by new NATO members, resulted in long-term stagnation of modernisation and the equipping of each country's armed forces. Many countries have not purchased artillery ammunition in decades."

The war in Ukraine is also prompting governments to think more laterally about the materiel they need, according to Wladek Rzycki, Infrastructure and Projects partner at CMS in Warsaw. ***"You have a very advanced conflict in the use of drones and guided missiles, as well as the heavy use of tanks and artillery,"*** he says. ***"This is shaping how contractors are creating and delivering products, and what governments buy."***

One company at the forefront of re-equipping CEE countries is the US aerospace and defence supplier Honeywell. ***"We're seeing a very intense race amongst the region's governments to improve armaments and armies,"*** says Piotr Marczuk, Honeywell's President and Director of Government Affairs CEE. In Poland, for example, ***"we see a huge wave of purchases across all military domains – fighter jets, helicopters, tanks, missiles and land vehicles. Abrams tanks purchased by the Polish Army will have the Honeywell engine at their heart. Without Honeywell technology, they will not drive."***

Honeywell also offers services guarding against cyber risks. ***"We've been operating our European Cyber Security Operation Centre in Romania for two years, servicing critical infrastructure and military customers,"*** says Marczuk. ***"Honeywell has three cyber ops centres around the world. The network has to work 24/7."***

New risks, new initiatives

Assisting innovation

Cyber security is one of many rapidly evolving concerns for military planners. NATO's recent Vilnius summit highlighted many new priorities, some aimed at hybrid threats. They include a centre for critical undersea infrastructure; centres of excellence for space and for climate change and security; new cyber defence initiatives and support capabilities; a commitment to protect energy infrastructure; strategies for quantum technologies, biotechnology and human enhancement; and plans for artificial intelligence and autonomy.

Such technologies are already shaping 21st-century conflict. In every case, they rely on digital applications and expertise.

Tech start-ups and other SMEs can find partnering with governments a very different experience from working with commercial partners. The slow pace of state-led defence procurement is particularly unsuited to new technology, where a rapidly evolving environment results in near-constant innovation and where a large number of potential contractors are small companies.

Says CMS partner Olga Belyakova, co-head of the CMS TMT in CEE: ***"One scenario is that private military and security companies will be significantly more agile than governments in their procurement of new technology. We may even see some of them combining – maybe even merging – with tech companies to provide specialist field and support services based on proprietary technology."***

Attempts to support defence start-ups include the NATO Innovation Fund, a €1 billion venture capital fund backed by 23 NATO nations including many in CEE. Described as 'the world's first multi-sovereign venture capital fund', this will provide patient capital for early-stage defence tech companies that are developing cutting-edge

solutions to critical defence and security challenges in any of the participating NATO countries.

Another NATO project is a start-up accelerator called Diana (Defence Innovation Accelerator for the North Atlantic). This focuses on technologies including AI, quantum computing and biotechnology. It gives innovators access to NATO resources including grant funding, acceleration services and pathways to adapt their tech for defence and security needs.

The EU is also encouraging defence SMEs. In 2022 the European Defence Fund announced €1.2 billion of funding for over 60 collaborative R&D projects, involving not only aircraft, tanks and ships but also technologies such as military cloud, AI, semiconductors, space and cyber warfare, and disruptive technologies including quantum computing and new materials. Over 40% of the entities participating in these projects are SMEs. A further €832m of funding was announced in 2023.

Private capital

Some start-ups are benefiting from the shifting investment strategies of venture capitalists. In the US, such investment in defence start-ups more than doubled between 2019 and 2023, reaching \$33 billion.

Sums in the EU are smaller, with investment more common in businesses developing dual-use technology. Nevertheless, there is a recognition that governments are newly willing to invest in defence and, in particular, in defence innovation.

There is also an increasing acceptance among ESG campaigners, some of whom previously opposed investments in military technology, that the 'social' element of ESG requires a society to protect its citizens against threats.

"Renewed interest in defence tech across CEE seems set to create a wave of investment," says Olga Belyakova, ***"In particular, the evolution of civilian technology will continue to benefit defence tech companies, not least in a wide range of cyber applications."***

"Renewed interest in defence tech across CEE seems set to create a wave of investment," "In particular, the evolution of civilian technology will continue to benefit defence tech companies, not least in a wide range of cyber applications."



Olga Belyakova
Partner, co-Head of TMT
in CEE, CMS

Keeping defence and tech together

In military life, as in commercial life, an array of legacy systems has to be managed. They are frequently indispensable, but also often incompatible with newer developments and sometimes with each other. Some have long-standing defects that are well-understood but also difficult to remedy.

New technologies offer the chance to create hybrid new-old platforms. Modifying the control systems of existing military equipment, for example, is capable of providing it with significant new functionality.

New tech can also enhance the connectivity of existing equipment, enabling it to integrate with new systems and operate more effectively alongside them.

New digital frontiers

Artificial intelligence is probably the most high-profile civilian digital technology that is being adapted for defence use. It is already becoming transformative in some military contexts, enabling large amounts of data to be processed and complex patterns analysed.

In the future, it is realistic to expect the development of fully autonomous weapons and vehicle systems, AI-enhanced command and control systems, AI-driven training systems, and the capability to analyse satellite imagery, troop movements and potential targets at unprecedented scale and speed. Other uses will include platform testing and scenario modelling, and 'human augmentation' – initially in powering augmented or virtual reality systems, but potentially in devices such as exoskeletons and implants.

AI also has huge potential to enhance cyber security in areas such as monitoring, threat detection and recovery (as well as, conversely, greatly enhancing the capacity and ability of cyber attackers). CEO of Grayscale AI (a company enabling fully autonomous drones using neuromorphic AI) Dragos Stanciu says: ***"There is a need in defence for innovative solutions that are able to operate in denied or contested environments (like inaccessibility of GPS signal). In the autonomy space, robotic platforms, such as aerial or underwater drones, need to be able to understand their surroundings by processing the data on the platform itself. Sending a lot of data to another point for analysis is problematic not only because of bandwidth issues, but also because of the risk of the data being intercepted and altered. Smaller,***

compact, and energy-efficient AI models are needed in order to analyse the data in real-time, at the edge, close to the sensors".

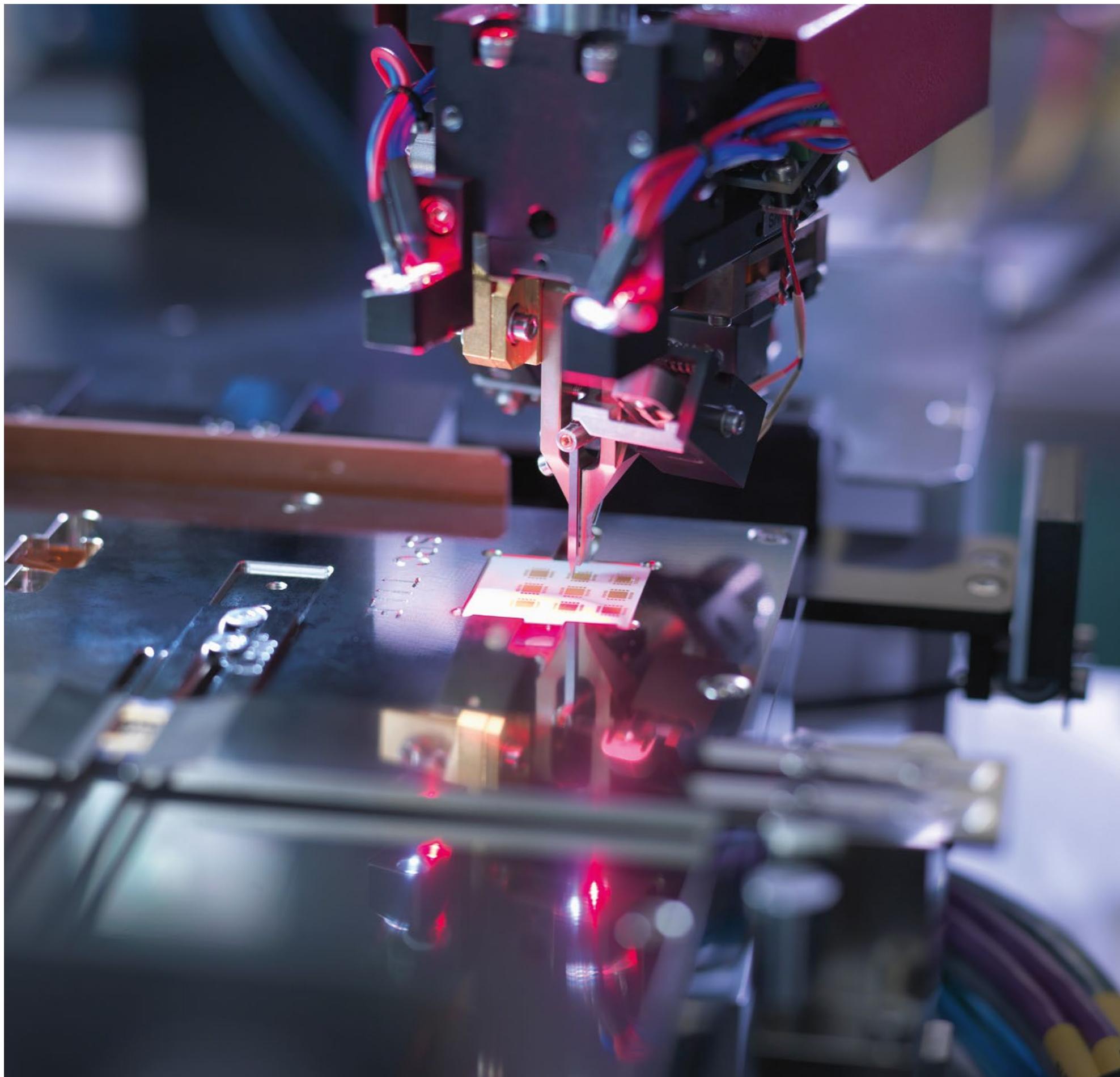
Other digital technologies are increasingly common in product development. For example, digital modelling and digital twinning are now invaluable in the development and refinement of military hardware, helping to eliminate design flaws and drastically cutting development time. Digital twinning can also greatly improve and accelerate the equipment maintenance cycle, and can be used as the basis for a range of training packages.

"There is a need in defence for innovative solutions that are able to operate in denied or contested environments (like inaccessibility of GPS signal). In the autonomy space, robotic platforms, such as aerial or underwater drones, need to be able to understand their surroundings by processing the data on the platform itself."



Dragos Stanciu
CEO of Grayscale AI

Cyber challenges



Soft targets

New forms of cyber attack are evolving, with a wider range of targets. According to the Microsoft Digital Defense Report 2023: ***"As the threat landscape evolves, we are seeing a blurring of lines between cyber operations, espionage, influence campaigns, and destructive attacks."***

Many attacks aim to extort money or steal data. But others seek to interfere in the political process, damage critical infrastructure, influence public opinion, cause economic harm or undermine civilian security.

In a sign of how seriously such attacks are viewed, NATO has publicly stated that hybrid actions or a cyber attack or series of attacks that 'reached the level' of an armed attack could lead to the invocation of Article 5 of the Washington Treaty, which would effectively put it on a war footing.

Private sector organisations are often seen as softer targets by hackers. The fact that much critical infrastructure is run by companies – and that companies are key to many important supply chains – is increasingly driving national security services, as well as bodies such as the EU and NATO, to offer such businesses cyber defence guidance and support, often on top of the support they may buy from IT security consultancies.

But businesses may also have a range of more purely commercial concerns. For example, if a cyber attack may be an act of war, is it covered by the war exclusions in cyber insurance policies? Have business secrets or IP been stolen? Has a data breach left the company liable to a fine from the regulator?

Answering such questions, which extend beyond the technical expertise needed to defend against cyber attacks, requires a different – but equally necessary – approach and skillset.

'A big warning'

While many cyber attacks have been unsuccessful, others have caused real damage. An attack on Kyivstar, Ukraine's biggest mobile and internet business, knocked out the service provided to 24 million users for several days in December 2023.

In addition, the attackers reportedly had undetected access to the company's systems for some time before they triggered the outage, which may have enabled them to gather intelligence or steal data.

Kyivstar had successfully repulsed hundreds of previous cyber assaults. And with the help of Ukraine's State Security Service (SBU), it appears to have defended itself successfully against a string of further attacks intended to extend the outage. But the incident is a reminder that, while most cyber attacks fail, a single security lapse or undetected weakness may be enough to let one succeed, potentially with serious consequences.

As the head of the SBU's cyber security department put it: ***"This attack is a big message, a big warning, not only to Ukraine, but for the whole CEE and even wider Western world to understand that no one is actually untouchable."***



Cyber solutions



If you follow a cyber security framework and think you are safe but don't know these new types of attack techniques, that's when big gaps may emerge in your cyber security defence. That can get pretty ugly, pretty fast.



Olav Østbye
CEO of O3 Cyber

Effective cyber security also requires continuous re-evaluation and improvement, as the scope and threats of cyber attacks evolve. This applies to governments, militaries and the private sector alike. Bear Midkiff argues that those companies which succeed will not apply the same configuration for more than six months to two years. The pace of technological change, he suggests, is simply too great.

According to Midkiff, ***No area requires more rapid change than cyber defence: communications infrastructure, distribution of data, command and control, and IT. Cyber experts have built their relationships on the IT model, which is based on teaming.*** As an example, he points to the NATO Cooperative Cyber Defence Centre of Excellence in Estonia. ***It is testament to the rapid evolution of the IT sector in the CEE region.***

This degree of vigilance and expertise can be challenging for even major tech companies and governments to maintain. For the average company, it may be genuinely daunting – especially where a business with little experience of these issues suddenly becomes an attractive target for would-be attackers.

A cyber security expert who collaborates closely with European clients to formulate their cyber security strategies, Olav Østbye is CEO of O3 Cyber. ***In the cloud, we see new attack techniques every week,*** he says. ***If you follow a cyber security framework and think you are safe but don't know these new types of attack techniques, that's when big gaps may emerge in your cyber security defence. That can get pretty ugly, pretty fast.***

There are major upsides to using the cloud securely, argues Østbye. ***In a cloud environment that's mature and configured by cloud security experts who are aware of these modern threats, then it's hard for an advanced adversary to attack you,*** he says. ***The cloud provider delivers a strong fundamental defence on their side, and your cloud security experts will cover the rest.***

In Europe, he sees an increasing move to the cloud. ***Companies traditionally had on-premise data centres, but they now want to utilise the speed, flexibility, and fundamental security benefits provided by the cloud.***

Stanciu adds: ***In the secure information sharing space, there is a need to find new ways of sharing data streams such as audio or video, in a secure and trusted fashion. Furthermore, these systems need to be robust against jamming and be able to provide reliability in complex environments such as dense urban environments. Quantum technologies are particularly of interest in this space.***

In the EU, legislation is bolstering cyber defence. The EU Cyber Resilience Act, set to be adopted soon, introduces cyber security requirements for connected devices, addressing potential vulnerabilities in both hardware and software.

The EU is also increasingly coordinating its cyber defence actions with NATO, which aims actively to deter, defend against and counter the full spectrum of cyber threats, not only during conflicts and crises but also during peacetime. One aspect of its role is helping key businesses and other organisations in member states to defend themselves from cyber attacks.

One important challenge, adds Midkiff, is the diminishing distinction between military and civilian targets. ***"Is a cyber attack against a country's major employer an act of war?" he asks. "How do we protect our infrastructure in the same way that we protect our borders? What is the line between constant vigilance and active conflict? Hybrid warfare and criminal networks blur the lines."***



Civilian or military?

Blurred lines are not just a feature of cyber warfare. All modern military organisations use non-military systems alongside their military technology. In NATO's words:

"The evolving security environment increasingly requires ... a structured and tailored approach that uses non-military and military tools in a deliberate, coherent, and sustained manner, throughout the full spectrum of peace, crisis and conflict."

Some non-military tools find prominent applications in hybrid war. But others feature dual-use technology, capable of being employed for both kinetic warfare and peaceful purposes.

Systems designed for civilian purposes – ranging from weather forecasting and geolocation apps to mobile phones and digital imaging – can be readily adapted for battlefield use. Specialist sensors and robotics may easily be modified to meet military requirements.

In some areas, the distinction between civilian and military functions has been blurred even further. The internet and social media have themselves become dual-use technologies, enabling greatly increased civilian participation in various conflicts.



Public and private

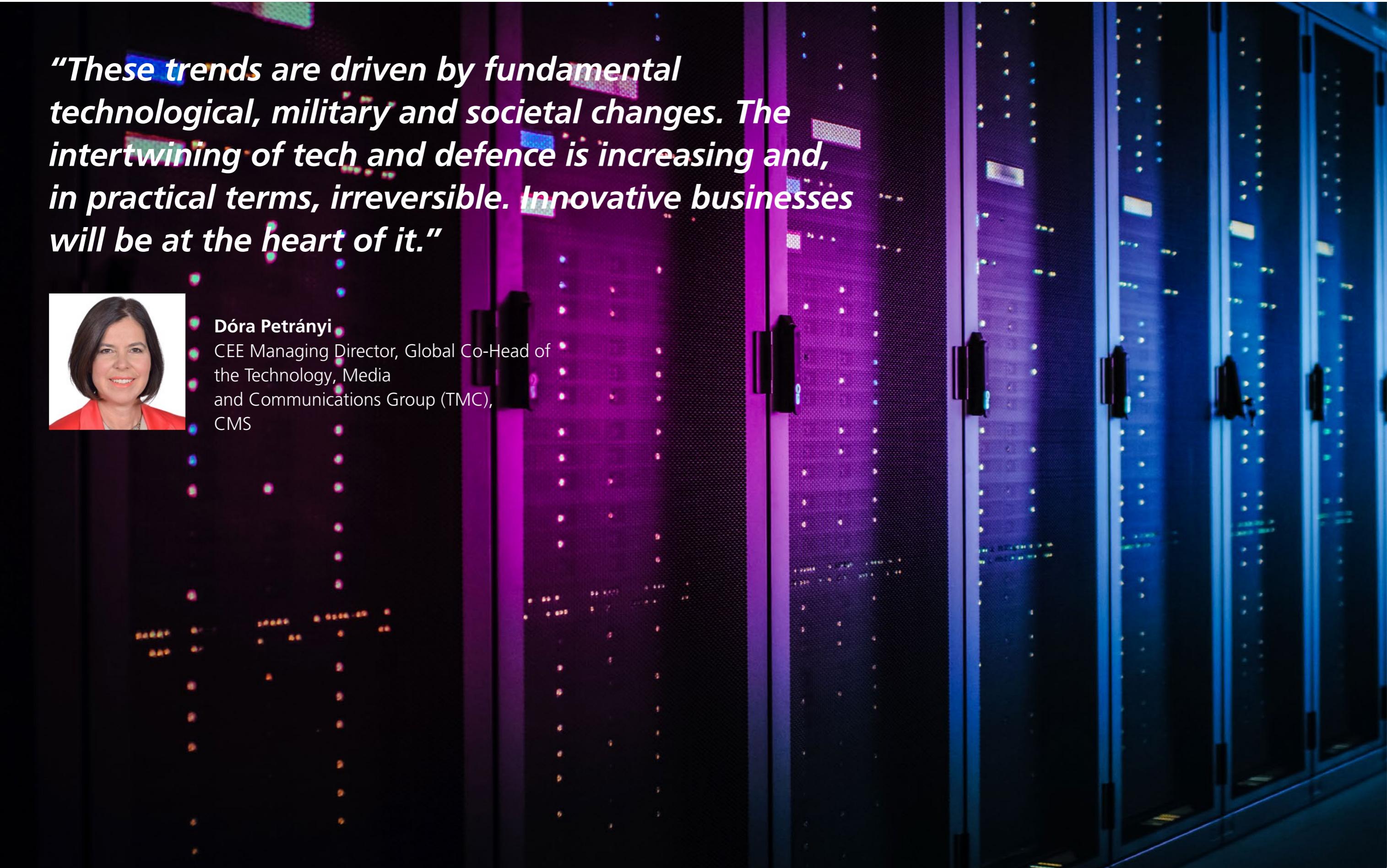
Innovative dual-use technologies are of increasing interest to military leaders in a more conventional sense. For many years private sector innovation in most countries has been faster and better funded than state-run R&D. Technology that may be vital in future military applications – such as artificial intelligence – is thus now controlled by businesses rather than governments. Many of these businesses are not part of the traditional defence establishment but have grown out of the ‘move fast and break things’ ecosystem associated with Silicon Valley. Others are corporate giants of the modern world, with massive R&D capacity and assets.

The cyber security resources of a business like Microsoft, for example, easily outstrip those of most governments. The supply chain expertise and infrastructure of Amazon are superior to those of many armed forces. And the satellite constellations of private sector providers – notably SpaceX’s Starlink, but also Eutelsat OneWeb and others – now account for the bulk of technology in earth orbit.

Such businesses reminds us that not all innovative defence contractors are SMEs. Nor are they all focused largely on defence – although, for some, defence is a significant business line.



Defending the future



"These trends are driven by fundamental technological, military and societal changes. The intertwining of tech and defence is increasing and, in practical terms, irreversible. Innovative businesses will be at the heart of it."



Dóra Petrányi

CEE Managing Director, Global Co-Head of the Technology, Media and Communications Group (TMC), CMS

Defence spending will continue to rise as governments respond to geopolitical concerns. The apparently unstoppable growth of hybrid warfare will see similar growth in cyber security and other non-kinetic defence systems, in both the public and private realms.

The young people who serve in today's wars are digital natives. Increasingly, so are the civilians they fight to protect. Even the most conservative military establishments with the most intractable legacy platforms will ultimately adopt fully digital defence systems, because the world in which they strive to prevail has itself gone digital.

Says CMS partner, Dóra Petrányi, CEE Managing Director, Global Co-Head of the TMC Group ***"These trends are driven by fundamental technological, military and societal changes. The intertwining of tech and defence is increasing and, in practical terms, irreversible. Innovative businesses will be at the heart of it."***

New tech, new threats

But emerging and disruptive defence technologies may not always lead to increased security. Hybrid wars now have low barriers to entry, especially in the cyber realm. Even 'hard' new-tech weapons like drones are increasingly available to smaller non-state actors. (Drones are already commonly used for drug smuggling, and drug cartels in Mexico have been deploying them as weapons against both other cartels and law enforcement agencies.) The division between armed militias and criminal gangs is becoming more porous, where societal and technological developments enable them to occupy both roles. And regimes seeking deniability will continue to use such entities as proxies.

This combination of innovation and uncertainty will continue to fuel investment in a variety of defence systems, not only in the public realm but also among businesses that may be targets in hybrid warfare. If they are not prepared to become participants in the cyber security arms race –adopting and continually upgrading cyber defences – they risk becoming its casualties.

A strong future for defence businesses

"Defence tech had a relatively low profile in CEE," says CMS partner , Eva Talmaci, co-head of the CMS TMC group in CEE. *"With recent events prompting increased government purchasing, the sector is set to grow in CEE, presenting opportunities not just for tech innovation but for financing and strategic M&A."*

While SMEs may participate fully in developing innovative tech, the sector's larger and more richly resourced players are more likely to offer the comprehensive solutions needed to integrate this tech with existing systems and manage its cross-platform operationalisation. But some SMEs will themselves grow into such backbone businesses.

"Like CEE governments, the EU is moving ever more decisively towards pro-European procurement, looking to boost continental defence champions and hubs," says Rzycki. *"Some of today's defence SMEs and start-ups will in time be among those champions and future sector leaders,"* says Belyakova.

"Like CEE governments, the EU is moving ever more decisively towards pro-European procurement, looking to boost continental defence champions and hubs"



Wladek Rzycki
Partner
Infrastructure and Projects Group
CMS

"Defence tech had a relatively low profile in CEE," "With recent events prompting increased government purchasing, the sector is set to grow in CEE, presenting opportunities not just for tech innovation but for financing and strategic M&A."



Eva Talmaci
Partner
Co-Head of CEE TMT, CMS

Talk through your digital strategy with us

If you would like to consult on or stress-test your business' digital strategy with your local CMS experts, please do get in touch with us.

CEE



Dóra Petrányi
Partner, CEE Managing Director,
Global Co-Head of the TMC, CMS
T +36 1 483 4820
E dora.petranyi@cms-cmno.com



Olga Belyakova
Partner, Co-Head of CEE TMT
T +380 44 391 7727
E olga.belyakova@cms-cmno.com



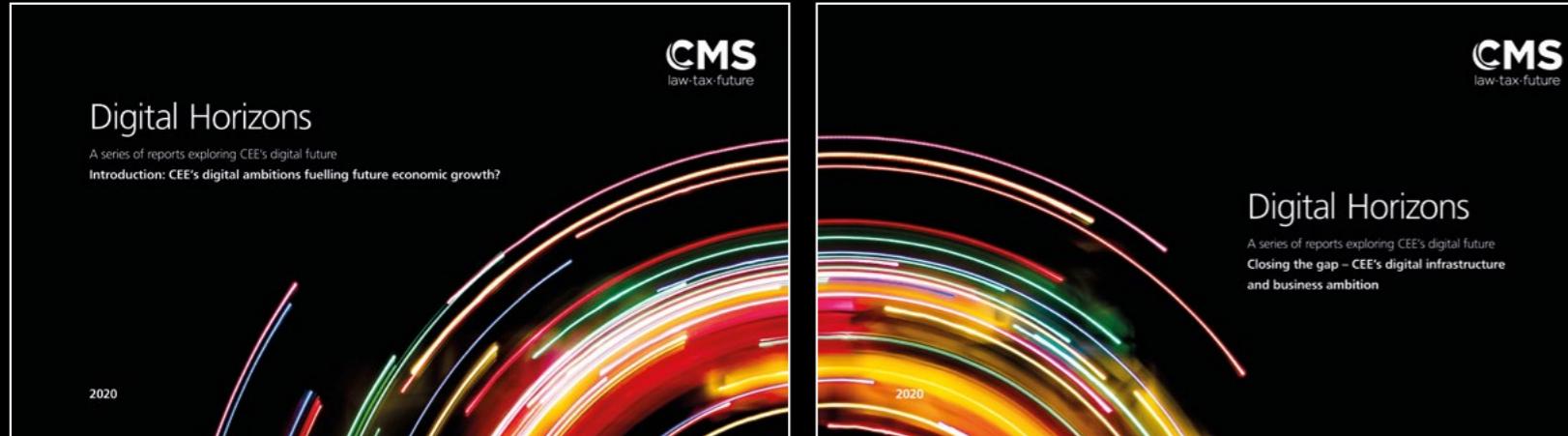
Eva Talmaci
Partner, Co-Head of CEE TMT
T +44 20 7367 2435
E eva.talmaci@cms-cmno.com



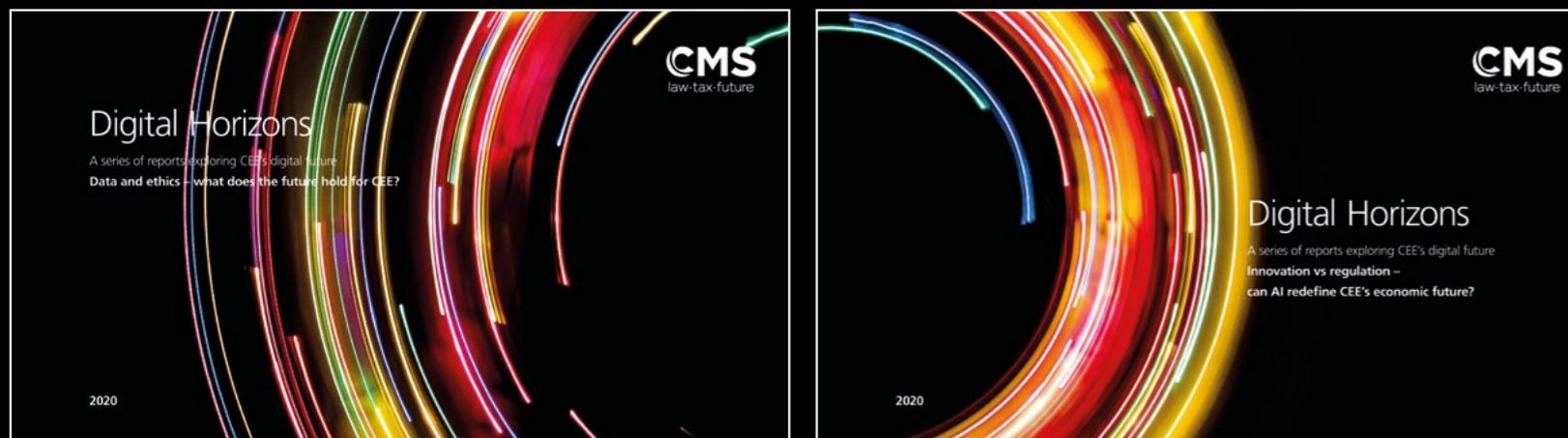
Wladek Rzycki
Partner, Infrastructure and Projects
T +48 22 520 56 97
E Wladek.Rzycki@cms-cmno.com



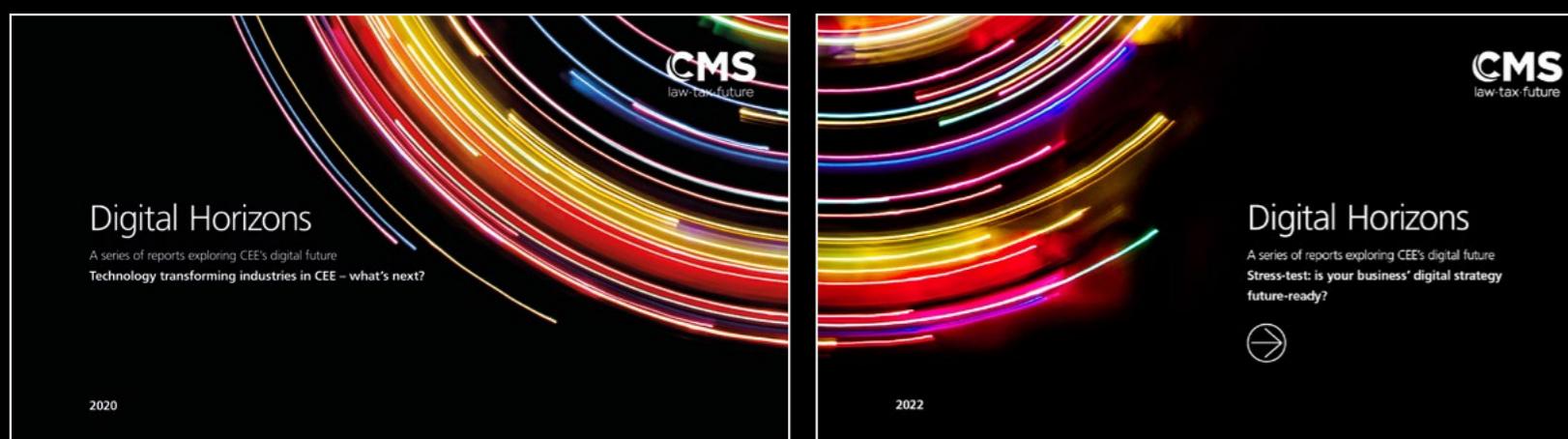
Digital Horizons: A series of reports exploring CEE's digital future



Read the rest of the Digital Horizons series [here](#):



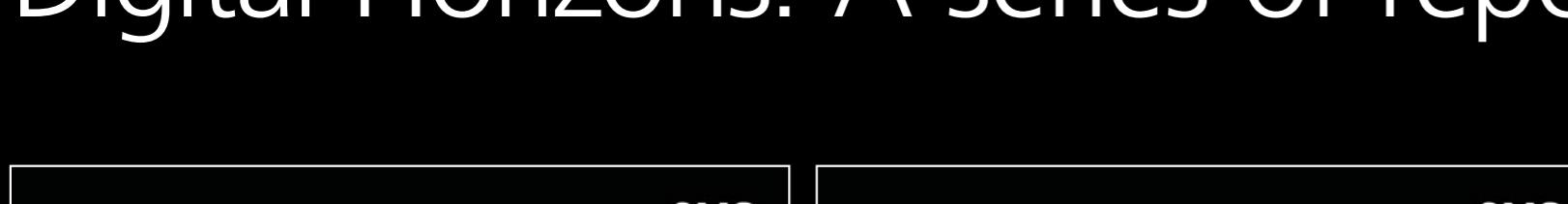
Introduction: CEE's digital ambitions fuelling future economic growth?



Closing the gap – CEE's digital infrastructure and business ambition



Data and ethics – what does the future hold for CEE?



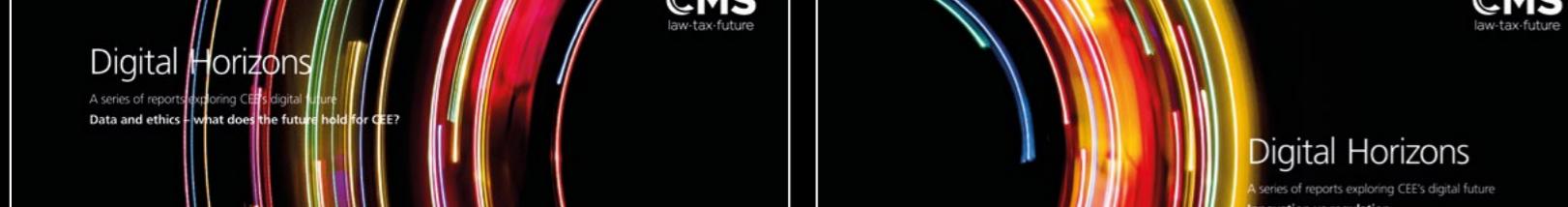
Innovation vs regulation – can AI redefine CEE's economic future?



Technology transforming industries in CEE – what's next?



Stress-test: is your business' digital strategy future-ready?



Data Centres – Scaling up in CEE



Digital regulation: a deeper dive into the DNA of the DMA and DSA





Your free online legal information service.

A subscription service for legal articles on a variety of topics delivered by email.

cms-lawnow.com

The information held in this publication is for general purposes and guidance only and does not purport to constitute legal or professional advice. It was prepared in co-operation with local attorneys.

CMS Legal Services EEIG (CMS EEIG) is a European Economic Interest Grouping that coordinates an organisation of independent law firms. CMS EEIG provides no client services. Such services are solely provided by CMS EEIG's member firms in their respective jurisdictions. CMS EEIG and each of its member firms are separate and legally distinct entities, and no such entity has any authority to bind any other. CMS EEIG and each member firm are liable only for their own acts or omissions and not those of each other. The brand name "CMS" and the term "firm" are used to refer to some or all of the member firms or their offices; details can be found under "legal information" in the footer of cms.law.

CMS locations:

Aberdeen, Abu Dhabi, Algiers, Amsterdam, Antwerp, Barcelona, Beijing, Beirut, Belgrade, Bergen, Berlin, Bogotá, Bratislava, Bristol, Brussels, Bucharest, Budapest, Casablanca, Cologne, Dubai, Duesseldorf, Edinburgh, Frankfurt, Funchal, Geneva, Glasgow, Hamburg, Hong Kong, Istanbul, Johannesburg, Kyiv, Leipzig, Lima, Lisbon, Ljubljana, London, Luanda, Luxembourg, Lyon, Madrid, Manchester, Mexico City, Milan, Mombasa, Monaco, Moscow, Munich, Muscat, Nairobi, Oslo, Paris, Podgorica, Poznan, Prague, Reading, Rio de Janeiro, Rome, Santiago de Chile, Sarajevo, Shanghai, Sheffield, Singapore, Skopje, Sofia, Stavanger, Strasbourg, Stuttgart, Tel Aviv, Tirana, Utrecht, Vienna, Warsaw, Zagreb and Zurich.