2025

WHO IS PROTECTING EUROPE'S FUTURE?

The State of Defense and Cybersecurity Tech in CEE

THE RECURSIVE
STORIES SHAPE STORIES

wiser

CONTENTS

Introduction & Executive Summary 1
Europe: Preparing for War to Keep Peace 10
Sectors Overview 19
Wiser Technology: Interoperability by Design 29
Navigating the Dual-Use Dilemma 33
Presto Tech Horizons: Investing in Strategic Infrastructure 39
Mappings of the CEE Companies 43
Methodology 44
CEE Overview: Defense and Dual Use 48
CEE Overview: Cybersecurity 51
- UKRAINE 54
- BULGARIA 55
- ROMANIA 56
- HUNGARY 57
- POLAND 58
- GREECE 59
- CROATIA 60
- SLOVENIA 61
- BALKANS 62
- SLOVAKIA 63
- CZECHIA 64
- ESTONIA 65
- LITHUANIA 66
- LATVIA 67

Special: Ukrainian Defense Tech in 2024 68
Tech, Not Men, on the Battlefield 77
Bronia.AI: Acoustic AI 80
Cyber Warfare: The New Battlefront 82
Pentest-Tools.com: Making Attackers Try Harder 89
Navigating Technologies in Cybersecurity 92
Plainsea: Building Continuous Security 100
Kikimora: AI agents in Cybersecurity 104
Warsaw Equity Group: Fueling Cybersecurity Scaleups in CEE 105
Special: Preparing for The Cyber Resilience Act 108
Nordic Recruitment & Consulting on Talents 115
Conclusion: Future Outlook 116

ABOUT US

THE RECURSIVE
STORIES SHAPE STORIES

The Recursive is an independent community-born online tech media focused on the emerging innovation and startup ecosystems in CEE.

AUTHORS OF THE REPORT

Ana Marija Kostanić

Editor-in-Chief | The Recursive

Teodora Atanasova

Tech Editor & Journalist | The Recursive

Etien Yovchev

Co-founder & Managing Partner | The Recursive

OUR PARTNERS

MAIN SPONSOR

wiser

STRATEGIC SPONSORS

PRESTO TECH HORIZONS

Warsaw Equity Group

Plainsea Cybersecurity Platform

Pentest Tools

STARTUP SPONSORS

BRONIA PROTECTING THE FUTURE

NORDIC RECRUITMENT & CONSULTING

Kikimora

PARTNERS

DEFENDER Your gateway to the world of Ukrainian Defence Tech

dealigence

EDTH European Defense Tech Hub

Invest in Bravery

MEDIA PARTNER

DATA PARTNER

NETWORK PARTNER

NETWORK PARTNER

INTRODUCTION & EXECUTIVE SUMMARY

Why this report – now?

The 2024 marked a historic peak in state-based conflicts. The Peace Research Institute Oslo (PRIO) reports there were 61 active conflicts across 36 countries – the highest number recorded since 1946. As a result, over 100 countries around the world raised their military spending, and the world military expenditure reached a whopping €2.35 trillion in 2024. But 2022 was pivotal for one specific war - the largest one in Europe since the second World War.

Drivers of defense technology demand

Europe's strategic landscape has been dramatically reshaped by Russia's invasion of Ukraine in February 2022. With the war in its third year, military expenditure kept rising across the continent, pushing European military spending beyond the level recorded at the end of the Cold War.

A pivotal driver of this increased spending – besides obvious conflicts, is Europe's heightened awareness of its military vulnerabilities exposed by those recent conflicts. The invasion of Ukraine revealed significant gaps in Europe's defense infrastructure, such as insufficient air defense systems, limited rapid deployment capabilities, and gaps in logistical and supply-chain resilience.

The advancement and proliferation of next-generation warfare technologies constitute another critical driver. Technological shifts in warfare witnessed in the Ukraine conflict demonstrate tactical advantages that traditional forces lack. The integration of artificial intelligence (AI), unmanned systems (drones), and analytic platforms into contemporary military operations has become imperative rather than optional.

Rising cybersecurity threats

However, military strategists and policymakers alike are re-evaluating their arsenals, knowing well that physical borders are no longer the only front lines; digital defenses are equally critical. Furthermore, cyberattacks could cause €9.09 trillion in damage annually through 2025, a 300 percent increase from 2015, according to McKinsey data.

Cyber threats have evolved from rare nuisances into persistent, sophisticated operations aimed squarely at governments, vital infrastructure, and major corporations. In 2023 alone, ENISA reported a nearly 40% year-on-year spike in cyber incidents targeting critical infrastructure, businesses, and state institutions.

In the most recent WEF Global Outlook, nearly 60% of organizations state that geopolitical tensions have affected their cybersecurity strategy. Geopolitical turmoil has also affected the perception of risks, with one in three CEOs citing cyber espionage and loss of sensitive information / intellectual property (IP) theft as their top concern, while 45% of cyber leaders are concerned about disruption of operations and business processes.

Besides all that, the need for cybersecurity is continuing to grow because of innovation in multiple technologies and economic sectors, from agritech to renewables to digital health. The changing business landscape requires increasingly diversified and vigorous cybersecurity solutions.

On top of that, the introduction of AI into the cyber battlefield has made threats both smarter and sneakier. Just as businesses harness AI to boost productivity, cybercriminals employ it to craft compellingly deceptive attacks.

Military and defense needs

Reflecting this increasingly tense environment, military efforts in the world have doubled. Ukraine became the world's largest importer of major arms in the 2020–2024 period, with its imports soaring nearly 100-fold compared to 2015–2019. This unprecedented demand has stressed global supply chains, created new public-private defense partnerships, and incentivized investment into emerging technologies.

Other CEE states are no exception. Poland, for instance, has increased its defense spending from 2.7% of GDP in 2022 to 4.2% in 2024, and this is projected to rise to 4.7% in 2025 — well above NATO's 2% guideline. Similarly, Romania, Estonia, and Latvia are all scaling up their military budgets in response to both Russian aggression and pressure to meet alliance obligations. This robust financial commitment is being channeled not just into traditional arms but also into cyber capabilities, missile defense systems, and force modernization.

Furthermore, NATO's enhanced forward presence, with its cyber-defense centers and frequent multinational exercises across the region, underscore the alliance's strategic pivot toward hybrid warfare readiness. Across the board, the emphasis is now on rapid deployability, interoperability, and battlefield digitization, meaning: real-time data integration, AI-assisted operations, and encrypted communications. The CEE region, once considered a security consumer, is quickly transforming into a security provider within NATO's eastern flank.

Regulatory and compliance pressure

Geopolitical developments have put the global IT operating model under enormous pressure in the past decade. UNCTAD's Global Cyberlaw Tracker shows 79% of countries in the world have their own data protection laws and privacy laws, which is creating considerable fragmentation.

In 2024, the European Union further intensified its cybersecurity regulatory framework with the introduction of the Cyber Resilience Act (CRA), complementing existing directives like NIS2 and the data protection mandates of the General Data Protection Regulation (GDPR). NIS2 aimed to harmonize cybersecurity practices across the EU, enabling a unified approach to digital resilience, and CRA addresses the previously inadequate cybersecurity standards in many digital products.

These goals are being met to varying degrees. The CRA may impose high compliance costs on SMEs, potentially stifling innovation, while strict requirements for vulnerability management and secure-by-design development could delay product releases and updates. Similarly, NIS2 poses implementation challenges across member states with varying capacities and could strain smaller organizations with its extensive compliance obligations.

Cybersecurity and advanced defense technologies have become indispensable elements of modern geopolitics. They represent crucial national imperatives for the CEE states, not merely to bolster defenses in the region, but to ensure Europe's stability and security in an increasingly uncertain geopolitical era.

Why does CEE matter?

There are various mappings and reports on the defense technology, dual-use, and cybersecurity innovation landscapes worldwide. None of them mapped Central and Eastern Europe (CEE) to its full extent, as they are usually focused on bigger markets – or use CEE just as a reference and comparison point. If we wanted to show what CEE has to offer, we figured The Recursive needs to do it.

We explored **19 CEE countries and their startup ecosystems** to gain a comprehensive understanding of how players in the area are supported in their innovation and business progress. Most importantly, we wanted to find out how they complement the joint pursuit of protecting Europe in the uncertain times to come.

Our research indicates that CEE is rapidly emerging as a significant contributor to the global defense technology and cybersecurity landscape. From mature ecosystems like Poland, the Czech Republic, and Estonia to high-potential front-runners such as Ukraine, Romania, and Bulgaria, the region showcases a promising mix of innovation, institutional support, and private investment.

Countries across the CEE are developing cutting-edge solutions in autonomous systems and dual-use technologies, while the cybersecurity sector reflects both legacy strengths and a fast-growing startup drive.

This overview captures the unique trajectories of CEE nations as they shape the future of security, both regionally and globally. In the following lines, you can read an overview of each ecosystem, while in the country profiles (See Full Contents), you can dive deeper into the details.

Bulgaria

Despite its smaller size, Bulgaria plays an active role in CEE's dual-use market. It is home to two of the top-funded companies in the region, Dronamics and EnduroSat, both with strong dual-use potential. The funding landscape is relatively balanced, with companies raising capital across Seed, Series A rounds, and through grants.

On the cybersecurity side, Bulgaria can also take pride in its good funding distribution. There are notable players at the Seed and Series A levels, with Alcatraz AI being among the top 10 funded cybersecurity startups in the entire region. Bulgaria may not have a large cybersecurity scene, but the ones that are present have great traction.

Romania

Romania is carving out a niche in the defense tech and dual-use ecosystem. The country is supported by four military academies, more than most CEE countries. InnovX–BCR, a Romanian accelerator backed by BCR bank, supports companies like Space Hub, which builds nanosatellites and launches them using repurposed Volkow missiles for LEO missions.

One of the cybersecurity giants in the region confirms that in every direction we look. In the top 5 by the number of cybersecurity startups and product companies, Romania also takes 2nd place in the number of full-time employees those companies have. A strong education in cybersecurity, with 28 affiliated university programs, fuels further growth in the domain. Meanwhile, the active presence of local investors, such as GapMinder Venture Partners, Early Game Ventures, and SeedBlink, gives them the much-needed boost that many countries in the region lack.

Hungary

Hungary's defense-tech startup ecosystem is growing steadily, driven by strong government backing. In 2023, Hungary signed an agreement to manufacture combat drones in cooperation with Israeli and German companies as part of an effort to grow and modernize its military and defense industry.

In cybersecurity, Hungary occupies a stable midfield position in terms of the number of startups and funding it has acquired. Pre-seed and seed rounds dominate, which is largely due to the fact that the domain has many new players rather than a lack of larger checks. Here, it is worth mentioning Hungarian SEON, founded in 2017, is the 6th top-funded cybersecurity company in the region (amongst much bigger and older players).

Greece

Greece is emerging as a strategic hub for defense tech and dual-use innovation in Southern Europe, with a focus on autonomous systems, AI-driven defense applications, and underwater intelligence solutions. Greece's defense budget for 2024 amounted to slightly over 3% of GDP; the country is reinforced by four national-level military academies. This momentum builds on the foundations of Greece's legacy defense-industrial players such as Hellenic Aerospace Industry, EAS, and Skaramangas Shipyards.

The cybersecurity industry in Greece is highly services-oriented, so it is no wonder that this CEE country has a few notable products from cybersecurity vendors. The majority of them were funded internally, some received grants, and VC funding was very seldom used. Following that, Greece has one of the largest pools of universities offering cybersecurity programs, 28 of them – with a strong vendor workforce. On the "true startup" side, things are a bit thin. However, Greece is home to one of the globally known players – Hack the Box, a cybersecurity training and simulation platform with 1015 full-time employees.

Poland

Poland stands out as one of the most advanced and heavily invested defense tech ecosystems in Central and Eastern Europe, with strong momentum across aerospace, AI-driven systems, and advanced sensing and communications hardware. The country has seen steady backing from key investors like Hard2beat and Space3ac. Its defense posture is reflected in a substantial 2024 defense budget of €34 billion, the highest in the EU (as a share of its GDP). Poland also benefits from a solid institutional base, with five national military academies.

A true cybersecurity startup nation, with 71 players, Poland tops the CEE country list. However, that doesn't translate to the 1st place in funding and full-time employees. Poland doesn't have 1000-employee players like Lithuania, Romania, or Slovakia. Instead, it has many smaller successful players and soon-to-be scaleups, operating so well that many of them are bootstrapped. That being said, Poland takes third place in funding and boasts 14 companies that have accumulated total funding above €5 million.

Croatia & Slovenia

Croatia and Slovenia represent two emerging but relatively small players in the CEE defense tech landscape, each with unique areas of specialization and over 200 full-time employees in the defense and dual-use sectors.

With one military academy offering a tech-focused curriculum, both ecosystems are positioned for gradual growth, though further development will likely depend on stronger domestic investment and institutional support.

Small cybersecurity markets with a significant presence, thanks to two crucial players. Croatia's Reversing Labs and Slovenian HYCU are in a league of their own. Both employ over 200 people, with Series B funding exceeding € 50 million. Globally recognized, these companies may be the outliers, but they prove why the CEE region cannot be ignored.

Balkans

The Western Balkans, comprising Kosovo, Albania, Montenegro, North Macedonia, Bosnia and Herzegovina, and Serbia, host a small cluster of defense and dual-use startups. Across the region, eight companies are actively working on defense technologies in AI and machine learning, autonomous systems, and embedded hardware. The ecosystem remains in its early stages and is fragmented, with opportunities for growth through regional cooperation and greater alignment of investment. Despite these challenges, defense tech in the region is gradually advancing, propelled by rising security demands, technological ambition, and strategic alignment with NATO standards.

In cybersecurity, most companies from the Balkans group are based in Serbia, with Albania and Montenegro having one representative each. Balkan startup ecosystems are still maturing, and this is particularly evident in cybersecurity. In terms of education, though, they amass 30 universities with cybersecurity curricula, but most of those graduates end up in ICT services.

Ukraine

Ukraine has rapidly become one of the most active and strategically significant defense tech ecosystems in Europe, driven by wartime necessity. With startups operating across drone systems, electronic warfare, and robotics, the country is witnessing a boom in early-stage activity. Key investors include the Nezlamni Fund and SMRK VC. Ukraine's 2024 defense budget is approximately 34% of its GDP, a proportion unparalleled in Europe. While not a NATO member, Ukraine is a long-standing partner in NATO programs and benefits from extensive bilateral military assistance from the U.S., UK, and EU. Many startups remain undisclosed in public databases due to the sensitive nature of defense innovation during wartime.

With a strong ICT industry overall, Ukraine's cybersecurity sector is also gaining traction. We mapped 18 companies focusing primarily on AI-driven threat intelligence, identity & access management (IAM) and blockchain cybersecurity. The first place that Ukraine deserves, by all means, is for education, with an astonishing 41 universities offering cybersecurity-related programs.

Slovakia

Slovakia is quietly cultivating a high-potential defense and dual-use tech ecosystem. With 10 active startups and total funding nearing €158 million, the sector has gained momentum in recent years. InoBat, in particular, has positioned Slovakia as a regional hub for advanced battery technology with applications across defense and aerospace. In summary, Slovakia's defense innovation landscape is modest in size but increasingly strategic in focus.

If we exclude the major legacy player, ESET, Slovakia isn't at the top of the cybersecurity lists in our research. However, there are signals it has a good opportunity to establish itself more in the cybersecurity domain. There may not be notable mid-players, but there are interesting early-stage stars, half of which are bootstrapped.

The Czech Republic

The Czech Republic is emerging as a niche player in the European defense tech landscape, with strengths in immersive simulation, space analytics, and drone traffic management. Support from local institutions like ESA BIC Czech Republic and CzechInvest has helped nurture early-stage innovation, particularly in dual-use technologies. Its focus on next-generation training and aerospace technologies reflects a steady contribution to broader European security and defense efforts.

One of the true cybersecurity hubs of the region, The Czech Republic boasts a considerable number of startups in the industry. The distribution of investments isn't concentrated in one or just a few big players; instead, we see a good number of early-stage players ready to reach the growth level. Our research shows that the Czech Republic has a strong continuity of innovation and investment in the industry, making it, alongside Poland, one of the most mature cybersecurity ecosystems in the region.

Estonia

Estonia has developed a notably agile defense tech ecosystem, with 13 active startups working across autonomous systems, secure communications, and mission control platforms. With total funding reaching nearly €38 million, the sector has experienced increasing activity in recent years, supported by institutions such as ESA BIC Estonia. The country has witnessed a significant development as defense conglomerate EDGE has acquired a major stake in Estonia's Milrem Robotics. This transaction marks the largest foreign investment ever made in Estonia's defense industry.

The region's startup star proves its worth in many domains, but particularly in cybersecurity. With 44 startups, it takes the lead in our research for the number of players. It is one of the best investment distributions in the region, featuring a handful of companies that have been bootstrapped. Strong ecosystem builders and investors, such as Startup Wise Guys, alongside startup-focused policies and administration, keep Estonia above the regional and European average.

Latvia

The country has witnessed gradual development in its defense sector, supported by a 2024 defense budget of over 3% of GDP. Latvia maintains international cooperation through frameworks such as the EU CSDP, PESCO, NB8, and partnerships with Nordic countries, the U.S., and its Baltic neighbours. The local defense startup ecosystem remains small but active.

Latvia doesn’t have a plethora of startups to showcase in the cybersecurity realm. However, the standout company, Regula, makes up for it. This bootstrapped provider of forensic and biometric authentication tools is used by law enforcement and border agencies worldwide. With another bootstrapped rising star, Entangle, it only proves the grit that founders from underdeveloped startup ecosystems have.

Lithuania

One of the most intriguing features of Lithuania’s defense-tech startup ecosystem is its purpose-built sovereign VC fund, Coinvest Capital, launched in early 2023 and uniquely empowered to invest directly in pure defense technologies, without requiring civilian dual-use applications. This may position Lithuania as one of Europe’s leading innovation hubs in military-grade deep tech. Most of the startup are currently in their seed stage.

Home to one of the region’s cybersecurity giants, Nord Security has put great foundations for the industry. There are a few notable startups in the early stages who will hopefully continue the good legacy. The majority of Lithuanian cybersecurity startups and product companies are either bootstrapped or at the seed stage.


EUROPE IS
PREPARING FOR WAR
TO KEEP THE PEACE

Europe: Preparing for War to Keep the Peace

Author: Teodora Atanasova

In the early hours of a February dawn, Serhii and Olena wake to the sound of air-raid sirens in their Kyiv apartment. Holding their newborn and helping their three-year-old out of bed, they quickly realize this is not a routine alert; these are coordinated, targeted strikes. They rush to the bathroom, as they don't have a basement – the only space that could serve as a "two-walls-rule" shelter in this situation. *They know this won't be the last night they experience something like this.*

Scenes like these became routine across Ukraine, reaching every corner of the country.

The full-scale Russian invasion of Ukraine, starting in February 2022, marked the largest military assault on a European state since World War II. Towns and cities across the country became front line battlegrounds. Civilians were not spared – train stations, hospitals, apartment buildings, and energy plants were struck with increasing frequency. By the end of 2022, tens of thousands had been killed, millions displaced, and Europe had entered a new and uncertain era.

For decades, the continent had enjoyed relative peace and the belief that large-scale war in Europe was a thing of the past. Germany reversed decades of defense policy by announcing a €100 billion military investment package.[1] Finland and Sweden, historically neutral, applied for NATO membership.[2] Eastern European nations, once considered a geopolitical "buffer zone", now find themselves on the front lines of a new world order.

And yet, even as military spending increases and security doctrines are rewritten, one question remains especially important: ***Would that be enough?***

In June 2025, Russia launched one of the most intense missile and drone attacks since the beginning of the war, targeting Kyiv and other cities with hundreds of drones as well as ballistic and hypersonic missiles.[3] The message is unmistakable: the war is not "frozen," nor is it winding down. It is evolving.

Now, it's time for Europe to understand this: peace is not a permanent condition. It is something to be maintained. The question is not whether conflict is possible, but how long Europe has to get ready for what comes next.

Europe's readiness

The so-called "peace dividend" led most Western countries to downsize their militaries and shift their focus to counterterrorism operations instead.[4]

However, the war in Ukraine has exposed the flaws in this approach.

Marijn Markus is a Dutch data scientist known for his data-driven analyses of Russian propaganda on LinkedIn, with the aim to combat disinformation and maintain global attention on the conflict. In a recent conversation with The Recursive, he points out that “the European armies were built for peacekeeping, not for fighting peer adversaries. Fixing that means retraining forces, expanding reserves, and rebuilding the kind of Cold War-style readiness that’s deeply unpopular with voters”. He acknowledges that gaining public support for these measures across Europe will be a major challenge.

“The good news?,” Markus adds. “The money, the talent, and the tech all exist within Europe.”

Indeed, Europe collectively commands significant economic power, with the EU’s combined GDP exceeding €15.8 trillion.[5] This financial strength could provide a solid foundation to fund military modernization and research initiatives. But time is slipping away, and the gaps that should have been addressed sooner are becoming increasingly apparent.

What were the setbacks, and why didn’t Europe spot the threat years earlier, one might ask? Looking back, the 2014 NATO Summit in Wales marked a turning point in the alliance’s strategic posture. In response to Russia’s annexation of Crimea, NATO leaders agreed that each member state should aim to spend at least 2 percent of its GDP on defense within a decade.[6] Yet nearly eleven years later, many countries still fall short of that target.

The annexation of Crimea was not the first red flag for Russia becoming a major threat for the West. At the 2007 Munich Security Conference, Vladimir Putin openly cautioned against NATO’s eastward expansion, calling it a direct threat to Russian security.[7] The following year, tensions boiled over when Russia launched a military invasion into Georgia. It was Moscow’s first major military operation beyond its borders since the Cold War.[8]

What was Europe, particularly the EU, doing at this time? Even though some sanctions were imposed after 2014, the EU continued to strengthen its economic ties with Russia, increasing the alliance’s dependence on Russian gas.[9] Just months later, in June 2015, Nord Stream 2 was announced, supported primarily by Germany and a consortium of European energy firms – a proposed gas pipeline linking Russia and Germany through the Baltic Sea. This pipeline would have allowed the Kremlin to bypass Ukraine’s existing transit network entirely, costing Ukraine billions in annual transit fees and removing a key leverage point that helped deter further Russian military intervention.[10]

Even though the pipeline remained non-operational, as of 2021 the EU imported more than 40% of its total gas consumption from Russia.[11] One might ask: had Europe truly identified the threat and taken the necessary early measures in response? So far, the record suggests otherwise.

The 2025

European institutions have started to show a growing awareness of security challenges, with a focus on the continent's defense gaps. Martin Jõesaar, EU Defence Innovation Office in Kyiv, elaborates more on Europe's readiness: *"Is Europe ready? Maybe. It depends on what the conflict would look like. Are we overconfident? Possibly. A more interesting question for me is: are we moving fast enough? Things are definitely accelerating, and we need to catch up. Procurement systems, development projects – all of that needs to head in the right direction, and quickly."*

The European Commission's ReArm Europe Plan/Readiness 2030, presented in March 2025, proposes to leverage over €800 billion in defense spending. Its main goal: to strengthen Europe's defense capabilities over the next five years and ensure collective readiness in the face of evolving threats.[12]

"I hear generals talk about five-year innovation plans. But let's be honest – we don't have five years. The current technological gaps in Western militaries – especially those revealed by the war in Ukraine – can be realistically addressed, but not overnight," says Marijn Marcus.

In Germany, for example, the Bundeswehr's rapid procurement of Leopard 2A8 tanks and Patriot PAC-3 missile systems under the €100 billion Zeitenwende package was indispensable.[13] However, these efforts only began to take shape after the military had endured years of insufficient investment.

The Recursive spoke to Kate McKenna, an authorized representative and strategic consultant for Ukraine's Defense and Intelligence sector. Appointed by senior Ukrainian defense leadership, McKenna negotiates with global stakeholders to secure advanced weaponry, munitions, cyber defense technologies, and funding to strengthen national security.

"Europe is not prepared or ready to defend itself. The defense procurement processes in the West, particularly in Germany, are flawed and not operating at the required pace. It is limited to Primes and lacks the innovative dynamism needed to create a modern warfare-ready military. Europe has outdated security frameworks and is slow to adapt to emerging technologies like drones and AI."

McKenna emphasizes that Europe still relies heavily on outdated military systems, with 50% of its land systems and 80% of land-based air systems dating back to before 1990, significantly limiting operational effectiveness.

"Its R&D investment is far lower than the U.S., with a €120 billion gap in 2023. Ultimately, Europe lags in drones, cyber defense, and space technologies, which are essential for modern warfare," explains McKenna.

"Germany's military lacks adequate air defenses against Russian hypersonic missiles, which could neutralize key infrastructure in Berlin or elsewhere in minutes," she adds.

Across the continent, Europe faces structural challenges that continue to drag down defense readiness. Jõesaar notes that while countries like Poland have begun strengthening their air defenses, overall progress across Europe remains uneven and too slow to keep pace with the growing complexity of modern security threats.

"Ukraine has excelled at rapidly training personnel and adapting on a large scale, driven by the immediate pressures of being at war. They have to adapt. On the European side, many people don't feel that same urgency. Some believe the threat from Russia is exaggerated. We're comfortable in our current reality, which may not reflect the true risks. The key question is whether we can adapt quickly enough. Ukraine has shown what's possible, but scaling those efforts in Europe is a much more complex task," Jõesaar adds.

France has long advocated for a more self-sufficient European defense industry. The country, too, has accelerated its military-programming law (Loi de Programmation Militaire, LPM) to allocate €413 billion by 2030 (40 percent more than its previous cycle) but this reprioritization comes after a decade of relative stagnation.[14]

In other words, France's lofty ambitions to regain "European strategic autonomy" will be undercut until these new platforms become operational – years behind where they should be today.[15]

McKenna also emphasizes that Poland, as a NATO front-line state, maintains a robust military force with more than 200,000 active personnel and modernized equipment and would likely offer significant resistance in the event of aggression.

"Poland is the only European NATO member capable of a decent defense. While NATO's rapid reaction forces (Very High Readiness Joint Task Force) can deploy within days, full mobilization of NATO's 3.5 million troops would take weeks to months," she explains.

Ukraine: The biggest testing field

For Europe, Ukraine's experience is not just instructive – it is essential. The country Ukraine acts as a geopolitical shield, absorbing the costs of conflict that would otherwise ripple further into the European Union.

"We need a new European security framework that incorporates Ukraine as a key player, given its practical experience and military resilience," says McKenna.

She explains that in her first career, she worked as a structured derivatives expert in capital markets, where she leveraged derivatives to mitigate geopolitical and market risks for a range of clients including sovereign entities, hedge funds, real estate fund managers, and international treasuries.

"One of the issues Europe faces when purchasing new technologies, such as drones, is that these systems are rapidly evolving, meaning a drone purchased today will likely be obsolete in six months' time. Additionally, it is impossible to build robust technology without testing it on the front lines. China, Iran, and North Korea are all learning and testing on Ukrainian soil. I suggest that derivatives can provide Europe with up-to-the-minute military technology when the need calls, and Ukraine gains the immediate funding it needs to defend itself and Europe," says McKenna.

Ukraine's economy shrank by over 29% in 2022 due to the war, with reconstruction costs now estimated at over €420 billion (World Bank, 2023) – nevertheless, the country has demonstrated remarkable grit throughout the conflict.[16]

Technologically, Ukraine's drone industry has seen a radical transformation: its domestic companies now manufacture roughly 1,500 tactical drones each year – more than 90% of them built entirely on Ukrainian soil.[17] For example, organizations like Aerorozvidka, a drone unit founded by IT specialists, developed the R18, a custom-built drone capable of carrying and deploying munitions. This UAV has been instrumental in reconnaissance and combat missions.

History is unfolding even as we write about it. On June 1st, Ukraine reportedly launched a dramatic long-range drone strike targeting Russian military bombers deep inside Siberia, damaging dozens of aircraft across multiple airbases thousands of kilometers from Ukrainian territory.[18] According to Ukrainian officials, the drones were covertly smuggled into Russia, concealed under the roofs of wooden sheds, and launched from trucks stationed near the targets.

The scope of the operation, known as "Spider Web", quickly became evident, with explosions reported across multiple time zones – from Murmansk in the Arctic north to the Amur region in the far east, more than 8,000 kilometers from Ukraine, damaging strategic bombers and early-warning planes.[19] The operation reportedly took over a year to plan and marks one of the most sophisticated drone attacks in modern warfare.

Indeed, defense today is not solely about weapons or military power.

Redefining security

At a time when many European citizens remain hesitant and critical about investments in the sector, the concept of defense is often misunderstood. It's not solely about tools of battlefield dominance – it's also about building resilience through infrastructure and modernizing outdated institutions. True security, as the war in Ukraine has shown, depends on much more than military strength – it requires effective strategy against hybrid threats, including cyberattacks, disinformation, energy coercion, and economic pressure. As the nature of conflict evolves, so too must our understanding of what it means to be prepared.

Disinformation campaigns have become a central component of modern hybrid warfare. Russia's Internet Research Agency (IRA), for example, operates troll farms and deploys bots across platforms such as Facebook, Twitter, and Reddit to push false narratives that erode faith in elections and governance.[20]

As McKenna points out, "Once the disinformation tap is turned on, any counter to it is like screaming into a raging thunderstorm. There are strategies and tactics that have some impact, like fact-checking and debunking. But that relies on people being open to and curious about the information they've just absorbed. Unfortunately, those who are targeted by these information warfare campaigns are often the least likely to visit a Fact-Checking site or read a media post debunking the narrative."

Beyond social media manipulation, recent campaigns like "Doppelgänger" have specifically targeted European publics by impersonating reputable outlets and spreading anti-Ukraine stories to weaken Western support for Kyiv.[21]

"We let ourselves be manipulated," says Markus. "It wasn't just propaganda – it was full-spectrum disinformation. Bots, troll farms, cyber campaigns. They hit us where we were most vulnerable: our democracies, our free press, our tendency toward self-doubt and self-blame. Messages like: 'NATO provoked this'; 'Ukraine is not our fight' – These weren't just opinions – they were planted, paid, amplified and weaponized. And while we debate and hold back, Russia advances," he adds.

Russia has significantly escalated its campaign of subversion throughout Europe, with operations led by its military intelligence agency, the GRU. According to a new CSIS database, the number of Russian attacks nearly tripled from 2023 to 2024.[22] Targets have included transportation systems, government institutions, key infrastructure, and industrial sites. Methods range from the use of explosives and physical tools (like anchors) to electronic warfare. Despite this surge, Western governments appear to still lack a cohesive and effective counterstrategy.

Waking up is not enough

"Democracy is a fragile gift that must be nurtured and protected by each generation."[23]

Waking up is not the same as being ready. The war in Ukraine has laid bare the uncomfortable truth: Europe cannot rely solely on legacy alliances and outdated doctrines to guarantee its security.

The burden of defense cannot fall on Kyiv alone. "The reality is, we're not prepared for that kind of large-scale attack. Ukraine has proven that these things can be done on a massive scale. And Russia continues pushing boundaries with their operations – it's almost weekly now," says Martin Jõesaar.

As Ukraine stands on the front lines, the battle for the future of democracy is being fought on its soil, and Europe is running out of excuses.

REFERENCES

1. “Germany Is Rebooting Its Military Because of Ukraine – And It’s a Big Deal” - TIME
2. https://time.com/6154487/german-military-expansion-ukraine
3. “NATO’s new defence plans will strengthen Allied deterrence and defence” – NATO
4. https://www.nato.int/cps/en/natohq/news_195468.htm
5. “Russia launches one of war’s largest air attacks on Kyiv, maternity ward hit in Odesa” – Reuters
6. https://www.reuters.com/world/russias-latest-drone-strikes-hit-kyiv-maternity-ward-odesa-ukraine-says-2025-06-10
7. “Europe’s security rethink: The age of peace is over” – Financial Times
8. https://www.ft.com/content/cf1638c4-45ed-4671-8c42-3136e7bda7d5
9. “European Union GDP - 2024 Data - 2025 Forecast” – Trading Economics
10. https://tradingeconomics.com/european-union/gdp
11. “Wales Summit Declaration” – NATO
12. https://www.nato.int/cps/en/natohq/official_texts_112964.htm
13. “A NATO Strategy for Countering Russia” – Atlantic Council
14. https://www.atlanticcouncil.org/in-depth-research-reports/issue-brief/issue-brief-a-nato-strategy-for-countering-russia
15. “The Enduring Impact of Ukraine’s Fight” – War Room – U.S. Army War College
16. https://warroom.armywarcollege.edu/articles/enduring-impact
17. “Europe’s Dependence on Russian Natural Gas: Perspectives and Recommendations for a Long-Term Strategy” – George C. Marshall European Center for Security Studies https://www.marshallcenter.org/en/publications/occasional-papers/europes-dependence-russian-natural-gas-perspectives-and-recommendations-long-term-strategy-0
18. “UK Defence Policy: An Introduction” – UK Parliament – House of Commons Library https://commonslibrary.parliament.uk/research-briefings/cbp-9462
19. “Focus – Reducing the EU’s dependence on imported fossil fuels” – European Commission https://commission.europa.eu/news-and-media/news/focus-reducing-eus-dependence-imported-fossil-fuels-2022-04-20_en
20. “European Defence Industry: Recent Developments” – European Parliamentary Research Service (EPRS) https://www.europarl.europa.eu/thinktank/en/document/EPRS_BRI%282025%29769566
21. “German budget committee clears over €6 billion in defence purchases, say sources” – Reuters https://www.reuters.com/world/europe/german-budget-committee-clears-over-6-bln-euros-defence-purchases-say-sources-2024-07-03
22. “Does France have what it takes to lead Europe’s defence initiatives?” – Euronews https://www.euronews.com/my-europe/2025/03/24/does-france-have-what-it-takes-to-lead-europes-defence-initiatives
23. “Europe’s defence push offers hope to France’s struggling car suppliers” – Reuters https://www.reuters.com/business/aerospace-defense/europes-defence-push-offers-hope-frances-struggling-car-suppliers-2025-03-20
24. “Updated Ukraine Recovery and Reconstruction Needs Assessment Released” – World Bank https://www.worldbank.org/en/news/press-release/2025/02/25/updated-ukraine-recovery-and-reconstruction-needs-assessment-released

25. “Ukraine to sharply raise purchases of home-produced FPV drones in 2025” – Reuters
https://www.reuters.com/business/aerospace-defense/ukraine-sharply-raise-purchases-home-produced-fpv-drones-2025-2025-03-10
26. “Why Europe is still not ready for war” – Financial Times
https://www.ft.com/content/ccd83e2a-521f-4e35-a5f0-2ec1ef63749e
27. “Ukraine releases new footage of drone attack on Russian strategic bombers” – Reuters
https://www.reuters.com/business/aerospace-defense/ukraine-releases-new-footage-drone-attack-russian-strategic-bombers-2025-06-04
28. “Russia’s disinformation playbook is poisoning AI systems – and grooming chatbots” – The Washington Post
https://www.washingtonpost.com/technology/2025/04/17/llm-poisoning-grooming-chatbots-russia
29. “Russian disinformation targets German election campaign, says think tank” – Reuters
https://www.reuters.com/world/europe/russian-disinformation-targets-german-election-campaign-says-think-tank-2025-01-20
30. “Russia’s Shadow War Against the West”
Center for Strategic and International Studies (CSIS)
https://www.csis.org/analysis/russias-shadow-war-against-west
31. “Twilight of Democracy: The Seductive Lure of Authoritarianism”
Anne Applebaum, Book

SECTORS
OVERVIEW

Where Demand Meets Supply

The twin domains of cybersecurity and defense technology are expanding in lock-step with the world's deteriorating threat environment. Ransomware has become the business model of organised crime, nation-states are probing critical infrastructure daily, and Russia's full-scale war in Ukraine has reminded governments that hard power still matters. These converging risks are pulling capital, talent and regulation into both markets at a pace unmatched since the early 2000s.

Exploding markets

Global picture. The commercial cybersecurity market is already comparable in size to the semiconductor sector. Its value is expected to rise from €264 billion in 2025 to €770 billion by 2034, driven by a strong compound annual growth rate (CAGR) of 12.6%.[1]

Among key market segments, cybersecurity services are anticipated to hold the largest share. In terms of security priorities, infrastructure protection is set to dominate, while Identity and Access Management (IAM) is projected to be the leading solution area.[2] Attack-surface expansion – cloud migration, industrial IoT and AI-generated code – keeps demand structurally ahead of supply, while stricter disclosure rules in the United States and the EU force even reluctant boards to budget for "zero-trust" architectures and managed detection services.

Venture investors are betting that the same digitalisation cycle will transform defense. Private funding for dual-use aerospace, autonomy and security software jumped 33% last year to about €27 billion, defying the wider venture-capital slump.[3] Governments are also leaning in: global military spending topped €2.4 trillion in 2024, and procurement budgets are being rewritten to privilege speed and software over long production runs of bespoke hardware.[4]

Europe's opportunity – and its gap. On the cyber side, the old continent's cybersecurity market size was valued at €66.1 billion in 2024.[5] Growth of 8.5% a year is healthy, yet still four percentage points behind the worldwide pace, chiefly because Europe's regulatory incentives and talent pool remain fragmented.

€100B

The **European cybersecurity market** is projected to reach over €100 billion by 2030, with CEE among the fastest-growing segments.

Twenty-seven transpositions of NIS 2 and DORA complicate selling across borders, and the region still depends on U.S. and Israeli vendors for advanced identity management, Secure Access Service Edge (SASE) and AI-enabled Extended Detection and Response (XDR). Closing that gap will depend on faster mutual recognition of cloud-trust labels, broader adoption of the EU Digital ID, and joint security-operations centers that pool scarce expertise.[6]

However, Europe's response to Russia's aggression shows how quickly the continent can move when incentives align. EU defense expenditures reached an estimated €326 billion in 2024 – more than 30% increase since 2021.[7]

As stated in the most recent report from the European Defence Agency, after a decade of under investment, it is essential that these increased resources are used wisely.[8] If available funds are invested strategically, the current spending increases could lay the foundation for a stronger European defense, not only addressing the gaps created by years of under expenditure but also preparing to meet future threats and challenges.

Central and Eastern Europe. The rearmament surge is most visible in the EU's eastern flank. Poland is vouching to dedicate more than 4% of GDP to defense in 2025, and Estonia aims to get there by 2026, with Greece (2.8% in 2024) and Latvia (2.9% in 2024) following close. In Table 1 you can see extrapolated CEE countries data from the European Defence Agency for the period of 2023/2024.[9] In total, listed CEE countries accounted for €54.58 billion of defense expenditures and invested €19.51 billion in defense.

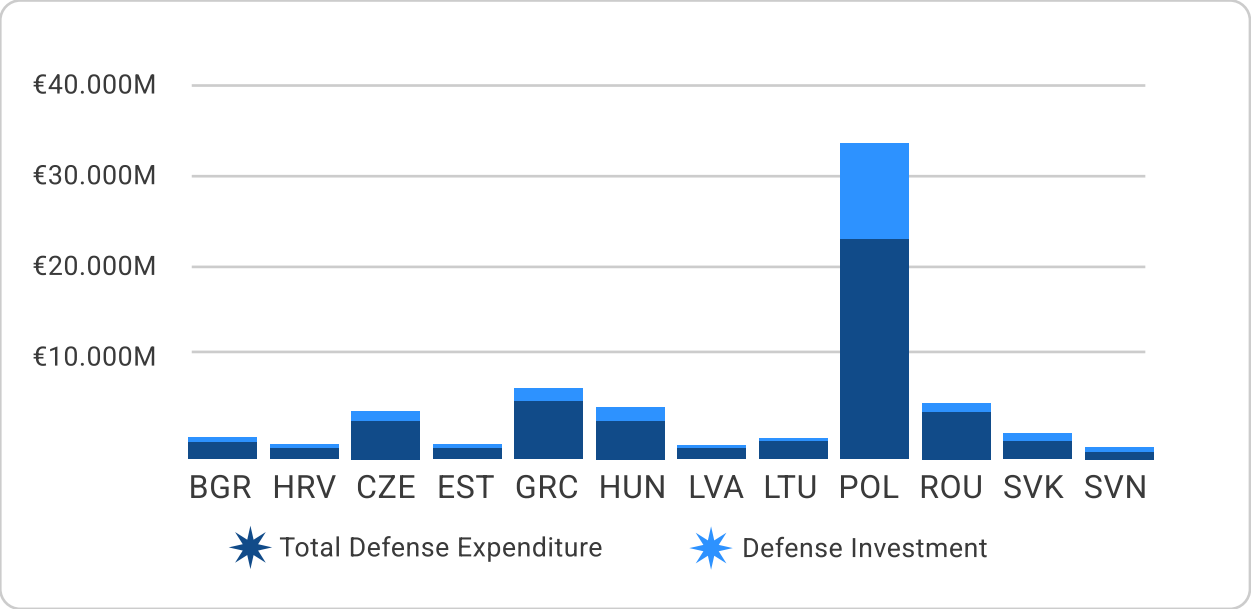


Table 1 - Defense Data, Comparison of Total Defense Expenditure vs Defense Investment
Source: European Defense Agency

When it comes to emerging startups bringing technology into the defense/dual-use sector, our research shows CEE is on a good trajectory with 170+ players. In comparison, Nordic's (Denmark, Sweden, Norway and Finland) account for 130+ startups in defense tech and dual use.

Ukraine is a different story – the country is home to early-stage defense tech startups, some with products already deployed on the battlefield or awaiting procurement, others with ready prototypes. We mapped 65 Ukrainian defense tech startups, most of them bootstrapped or having closed a seed round. Many more likely remain under the public radar for security reasons and do not appear in any official databases.

Traditional defense manufacturing is more concentrated in Western Europe, but countries in CEE are emerging as leaders in cybersecurity. With giants like Nord Security, Bitdefender and ESET, countries like Lithuania, Romania and Slovakia brought the region to global spotlight, while Estonia and Poland with an abundance of small and medium players are emerging as the region's cybersecurity hubs. CEE today is home to more than 270 cybersecurity startups and product companies.

Money is there

Cyberattacks, AI tools, and autonomous systems are no longer just supporting technologies – they're now central to national defense strategies. To keep up, governments around the world are looking beyond traditional contractors and turning to startups and private capital to develop and deploy advanced capabilities quickly.

CYBERSECURITY VC FUNDING[10]

2023 – €7.1B
2024 – €10.15B (+42%)

DEFENSE VC FUNDING (GLOBAL)[11]

2024 – €27.14B (+33%)

The U.S. leads in speed and in scale. The U.S. Defense Innovation Unit (DIU) has become a key part of how the Pentagon sources new technology. With a 2024 budget of nearly €1 billion and direct reporting to the Secretary of Defense, DIU helps turn commercial innovations into military tools. In 2023 alone, it received nearly 1,800 startup proposals which led to 90 prototype contracts covering areas like counter-drone systems, AI software, and space tech. Since 2016, the DIU has awarded 450 prototype contracts, which amounted to €4.84 billion contract ceiling awards and backed by €16.8 billion of private capital.[12]

This structure allows U.S. defense tech companies to grow fast. Startups like Anduril and Shield AI regularly raise hundreds of millions of dollars and move from concept to real-world deployment in just a few years. Government-led funding programs, like the Small Business Innovation Research (SBIR) initiative[13], also make it easier for nontraditional suppliers to break into the defense market.

In 2024, U.S. defense tech brought in about €2.6 billion via 102 deals, and Anduril's €1.3 billion Series F accounted for nearly half the total.[14]

Europe in coordination strikes bigger. Investment in European startups working on defense and related technologies jumped 24% in 2024 to record €4.55B, outpacing growth in venture capital for AI in the continent over the past two years.[15]

Most of the growth in the defense sector has come from startups focusing on solutions that help with awareness, understanding and decision making, as well as freedom of operations and mobility. The UK has attracted the most VC funding in Defence, Security and Resilience (DSR) sectors since 2019. However, Germany claimed the top spot in 2024, followed by the UK and France.

While Europe has traditionally lagged in speed against the US, it is making real progress through coordinated initiatives and stronger public-private partnerships.

- The European Defence Fund (EDF) allocated over €900 million in 2024 to 62 joint R&D projects.[16]
- NATO's Defence Innovation Accelerator (DIANA) selected 44 startups for its first cohort, while the €1 billion NATO Innovation Fund aims to crowd in private capital across dual-use domains.[17]
- In January 2024, the Defence Equity Facility was launched as a €175 million initiative, co-funded by €100 million from the EDF and €75 million from the EIF.[18]
- In January 2025, The European Commission adopted the 2025 Work Programme under the European Defence Fund (EDF), allocating €1.07 billion to collaborative defence R&D projects.[19]

Unlike defense tech, cybersecurity investments in Europe are not kicking highs. There was a notable decline in private investments for cybersecurity by the end of 2024, which is concerning as the EU already identified an annual venture capital gap in the sector of around €1.75 billion.[20] Also, there is the usual European "lack of late-stage funding" problem in this sector as well – more than half of all cybersecurity funding rounds in 2024 were seed or pre-seed.

CEE at the forefront. Driven by geopolitical circumstances and strategic imperatives, the CEE region has seen some increased investment activity in defense technology and cybersecurity innovation.

Our comprehensive mapping identified 174 defense and dual-use startups that cumulatively attracted €667.38 million throughout their lifespans, underscoring rapid growth despite the relatively young age of most companies.

One third of these startups got to the seed stage, while one third are at pre-seed or still relying on grants. Less than 20% of companies reached Series A and more. According to the Nordic defence tech report, between January 2023 and November 2024, CEE (with Baltics) amounted to €224.8 million worth of VC investments in defense and dual-use tech startups.[21]

When it comes to funding status by country; Slovakia, Poland and Bulgaria take the top three places, although in Slovakia 90% of investments can be attributed to InoBat's €137 million total funding. Estonia is also getting more active in the sector; not just because of the vicinity of the threats, but for the fact that the privately-funded groups in this Baltic nation are able to invest in purely military technologies. In contrast, in Poland – the region's biggest economy and major provider of military aid to Kyiv – many venture firms receive public funding which prevents them from directly financing military projects. Estonian initiatives include a €100 million public fund and Plural's private €800 million investment platform; overall the Estonian defense industry is aiming for €2 billion in revenue by 2030.[22] Similarly, the Czech Republic launched a €150 million defense-focused fund through Presto Ventures and CSG.[23]

In the cybersecurity domain, investing dynamics are somewhat different. The cybersecurity industry has a longer "startup" legacy and consistency of investing. However, there are quite a few established product companies that earned global recognition with no or just one funding round.

Looking at the total funding for the players we mapped in our research, Ukraine, Estonia and Poland are leading the pack with Greece and Czech Republic following closely. Distribution of investment is in favour of seed and pre-seed rounds, but there is also 19% of bootstrapped cybersecurity product companies and startups. This once again proves the resilience of the region as well as the quality and value its cybersecurity sector produces.

Talents paradox

Defense and cybersecurity organisations entered 2025 with a paradox: investment and demand have never been higher, yet the supply of people able to design, secure and build the next generation of systems has seldom been tighter. Across the world the cyber workforce is missing around 4.8 million practitioners, and defense primes on both sides of the Atlantic have tens of thousands of unfilled engineering, AI and advanced-manufacturing roles.[24]

In the United States the aerospace-defense sector employs about 2.2 million people, yet two-thirds of manufacturers still cite workforce quality as their top concern.[25] More than half a million cyber jobs remain open, many requiring high-level clearances that prolong hiring. The Pentagon's Cyber Workforce Strategy seeks to standardize roles, cut onboarding below 80 days and fund internal academies to grow talent.[26]

Europe starts from a smaller base but faces an even sharper climb. The defense industry supported 581,000 jobs in 2023. Meeting a 3% GDP defense target could mean 760,000 extra workers by 2035.[27] On the cyber end, in 2022, the shortage of cybersecurity professionals in the EU ranged between 260,000 and 500,000, while the EU's cybersecurity workforce needs were estimated at 883,000 professionals.[28]

Initiatives such as the EU Defence Industrial Strategy, the Union of Skills and the Assets+ alliance aim to give universities predictable demand, sponsor competitions like the European Defence Challenge and fund cross-border up-skilling, but they are only beginning to bite.

AI is both stress-multiplier and relief-valve. 91% of defense (security) leaders expect it to spawn new roles, and large language models already shorten Tier-1 triage by turning raw telemetry into plain English. Yet two-thirds of organizations under-invest in AI skills, stacking an "AI gap" atop the wider cyber shortfall.[29] The most successful employers roll out tools and training together, using AI tutors and simulated ranges so people move up the value chain rather than out of it.

CEE as the prime talent and testing hub. In our research with Dealigence platform, we noted more than 15,000 full-time employees working across 443 CEE companies in cybersecurity, defense and dual-use tech.

Lithuania, Romania, Slovakia and Greece are home to the biggest cybersecurity employees; but Poland, Estonia and Czechia have better distribution of the workforce amongst more companies. When it comes to cybersecurity curricula at the universities, Ukraine, Poland and Romania take the lead with more than 30 programs available in each country.

For defense tech, the mix is a bit different. Ukraine is far at the front, leaving the rest behind with only Estonia and Poland standing out. Their proximity to Ukraine allows close cooperation with front-line units to quickly test and tweak technology, which is an unprecedented opportunity for experts working or training to work in the field.

We already mentioned there is a significant cybersec and defense tech talent gap present in Europe, however – a rising number of top-tier AI professionals are joining defense tech startups motivated by mission-driven work and European autonomy—despite lower salaries than in the U.S.[30]

Looking closely at CEE, fortunately education supports the job market to a good extent. There are more than 240 universities with cybersecurity programs and 30+ military academies across the region offering some tech related curricula.

How is all of this helping innovation?

The flood of public money, venture capital, and accelerator programmes would matter little if it did not shorten the path from bright idea to deployed kit. Evidence from the last two years suggests the pipeline is indeed tightening – though at very different speeds on each side of the Atlantic.

In the United States, the Defence Innovation Unit (DIU) has begun to look less like an incubator and more like a production office. Cumulatively, from fiscal years 2016 through 2023, DIU has awarded 450 prototype OT contracts, with 51% of completed prototypes transitioning to production.[31]

The Pentagon's shift from traditional hardware-centric acquisition models to a more agile, software-centric approach, allows delivery of cutting-edge software solutions to warfighters faster and more effectively.[32] At the same time, major late-stage funding from firms like American Dynamism, Lux Capital, and Founders Fund helps startups survive long enough to meet classified system requirements.

Europe is moving in the same direction, but must knit 27 national systems into something that feels like a single market.

The first DIANA cohort, assembled in early 2025, is now working across 13 NATO test centres and beginning live trials with British, Polish and French units. Defense tech company Helsing's multiyear contracts – embedding real-time AI and sensor fusion in Bundeswehr armored platforms and contributing to the Franco-German Future Combat Air System (FCAS) – demonstrate that a European startup can secure prime-level mandates without relocating to California.[33]

Yet scaling remains painful: a company that pilots software (or hardware) in Latvia must still renegotiate standards, export licences and security clearances before selling the same code or hardware in Italy or Spain.

Central and Eastern Europe offer a glimpse of what a faster, less encumbered model might look like.

Polish and Baltic buyers, desperate for credible deterrence, test small-satellite ISR[34], counter-UAS jammers[35] and secure-mesh radios in weeks, not quarters. Ukrainian battlefield telemetry flows straight into regional cyber labs, giving engineers near-real-time insight into Russian tactics and malware. For investors, this compressed loop turns modest seed cheques into valuable validation, which can then be leveraged for pan-European grants and growth rounds.

Overall, the verdict is cautiously positive. In Washington, the combination of agile contracting and deep capital has collapsed innovation timelines to a pace that traditional primes now struggle to match.

Brussels and other EU capitals have not yet matched that speed, but new NATO testbeds, hefty defence rearmament budgets and a visible pipeline of flagship contracts are dissolving long-standing cultural taboos around military technology. The centre of gravity is drifting toward a blended model in which commercial scale, open architectures and battlefield-grade resilience are designed together from day one.

The strategy is working – not perfectly, but well enough that the question is no longer whether innovation will reach the front line, only how fast and under which flag.

REFERENCES

1. Cyber Security Market Size to Surpass USD 878.48 Bn By 2034 – Precedence Research https://www.precedenceresearch.com/cyber-security-market
2. Cyber Security Market Size, Share | Industry Report, 2030 – Grand View Research https://www.grandviewresearch.com/industry-analysis/cyber-security-market
3. Creating a Modernized Defense Technology Frontier – McKinsey https://www.mckinsey.com/industries/aerospace-and-defense/our-insights/creating-a-modernized-defense-technology-frontier
4. Unprecedented Rise in Global Military Expenditure; European and Middle East Spending Surges – SIPRI https://www.sipri.org/media/press-release/2025/unprecedented-rise-global-military-expenditure-european-and-middle-east-spending-surges
5. Europe Cybersecurity Market – IMARC Group https://www.imarcgroup.com/europe-cybersecurity-market
6. Cybersecurity Market Analysis and Recommendations v1.1 – ECSO https://ecs-org.eu/ecso-uploads/2024/12/ECSO-Cybersecurity-Market-Analysis-and-Recommendations-v1.1.pdf
7. EDA – Defence Data 2023–24 – European Defence Agency https://eda.europa.eu/docs/default-source/brochures/1eda---defence-data-23-24---web---v3.pdf
8. EDA Annual Report 2024 – European Defence Agency https://eda.europa.eu/publications-and-data/all-publications/annual-report-2024
9. Defence Data – European Defence Agency https://eda.europa.eu/publications-and-data/defence-data
10. Big Rounds Comeback 4Q EOY 2024 – Crunchbase News https://news.crunchbase.com/cybersecurity/big-rounds-comeback-4q-eoy-2024/
11. Creating a Modernized Defense Technology Frontier – McKinsey (duplicate) https://www.mckinsey.com/industries/aerospace-and-defense/our-insights/creating-a-modernized-defense-technology-frontier
12. FY23 Annual Report – Defense Innovation Unit (DIU) https://www.diu.mil/fy23
13. About SBIR – SBIR.gov https://www.sbir.gov/about
14. Defense Tech Funding Growth YIR 2024 – Crunchbase News https://news.crunchbase.com/venture/defense-tech-funding-growth-yir-2024/
15. Inaugural Dealroom and NATO Innovation Fund Report Reveals Record-Breaking Investing in Startups in European Defence, Security and Resilience Sector – NATO Innovation Fund https://www.nif.fund/news/inaugural-dealroom-and-nato-innovation-fund-report-reveals-record-breaking-investing-in-startups-in-european-defence-security-and-resilience-sector/
16. EDF 2024 Results – General Factsheet v7 – European Defence Fund https://defence-industry-space.ec.europa.eu/document/download/ad3cd2d3-591d-4587-95d9-2ab0c48ec255_en?filename=EDF%202024%20results%20-%20general%20factsheet%20v7.pdf
17. About NATO Innovation Fund – NATO Innovation Fund https://www.nif.fund/about/

18. Defence Equity Facility – European Investment Fund
https://www.eif.org/InvestEU/defence-equity-facility/index.htm
19. Strengthening European Defence through Innovation: Launch of EDF 2025 Work Programme (2025-02-07) – EUDIS
https://eudis.europa.eu/news/strengthening-european-defence-through-innovation-launch-edf-2025-work-programme-2025-02-07_en
20. European Cybersecurity Investment and M&A Quarterly Report – ECSO
https://ecs-org.eu/ecso-releases-european-cybersecurity-investment-and-ma-quarterly-report/
21. Nordic Defence – Danske Bank
https://danskebank.fi/-/media/danske-bank-com/pdf/fi/nordic-defence---danske-bank.pdf
22. Estonia's Tech investors take defence into their own hands as Russian threat looms – Reuters
https://www.reuters.com/business/aerospace-defense/estonias-tech-investors-take-defence-into-their-own-hands-russian-threat-looms-2025-02-21/
23. Czech Presto Ventures and Czechoslovak Group launch €150 m investment fund focused on security and defence tech – The Recursive
https://therecursive.com/czech-presto-ventures-and-czechoslovak-group-launch-e150m-investment-fund-focused-on-security-and-defence-tech/
24. ISC2 2024 Cybersecurity Workforce Study – ISC2
https://www.isc2.org/Insights/2024/10/ISC2-2024-Cybersecurity-Workforce-Study
25. 2024 Facts & Figures: American Aerospace and Defense Remains an Economic Powerhouse – AIA
https://www.aia-aerospace.org/news/2024-facts-figures-american-aerospace-and-defense-remains-an-economic-powerhouse/
26. Chief Digital & AI Officer Software Modernization Strategy – DOD CIO
https://dodcio.defense.gov/Portals/0/Documents/Library/CWF-Strategy.pdf
27. Skilled workers wanted: the EU's defence industry struggles to find the right talent – Euronews
https://www.euronews.com/my-europe/2025/02/26/skilled-workers-wanted-the-eus-defence-industry-struggles-to-find-the-right-talent
28. Mind the Cyber Skills Gap: a deep-dive – Digital Skills and Jobs Platform; EU
https://digital-skills-jobs.europa.eu/en/latest/briefs/mind-cyber-skills-gap-deep-dive
29. Global Cybersecurity Outlook 2025 – World Economic Forum
https://www.weforum.org/publications/global-cybersecurity-outlook-2025/
30. Mission Before Money: How Europe's Defence Startups Are Luring AI Talent (2025-04-30) – Reuters
https://www.reuters.com/business/mission-before-money-how-europes-defence-startups-are-luring-ai-talent-2025-04-30/
31. GAO-25-106856 Report – U.S. GAO
https://www.gao.gov/assets/gao-25-106856.pdf
32. Pentagon's Software Modernization Plan Targets Speed – GovCIO Media
https://govciomedia.com/pentagons-software-modernization-plan-targets-speed/
33. Helsing commissioned for AI backbone in FCAS – Helsing.ai
https://helsing.ai/newsroom/helsing-commissioned-for-ai-backbone-in-fcas
34. Polish satellite company collaborates with Polish military to deliver mobile ISR – National Defense Magazine
https://www.nationaldefensemagazine.org/articles/2024/9/5/polish-satellite-company-collaborates-with-polish-military-to-deliver-mobile-isr
35. NATO Needs a Hellscape: Defense at Replicator Speed – Atlantic Council https://www.atlanticcouncil.org/in-depth-research-reports/report/nato-needs-a-hellscape-defense-at-replicator-speed/

Interoperability by Design: Why NATO and EDF Trust Wiser Technology to Build Europe's Defense Software Backbone

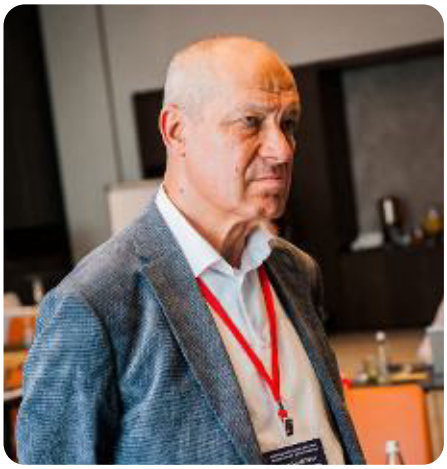
In the new era of defense, systems don't operate in silos. Communication, intelligence, decision-making, and action must be coordinated across domains in real-time. Whether it's Unmanned Aerial Vehicles transmitting surveillance zone video, AI parsing satellite images, or submarines relaying encrypted messages, the logic is the same: integration is no longer a feature, it's a core capability.

Wiser Technology, a software engineering company based in Sofia, Bulgaria, has quietly become one of the go-to players for delivering that integration. Over the past decade, the company has developed critical components for NATO and the European Defence Fund — not by building flashy tools but by making complex systems work together under military-grade requirements. Among Wiser's clients are also Airbus, Indra, Thales, Leonardo, Rheinmetall Group, and other industry leaders.

Their focus: real-time operations, interoperability, and full-lifecycle traceability.

From one NATO module to a portfolio of defense systems

Wiser's entrance into defense came in 2010 when it joined the NATO Alliance Ground Surveillance (AGS) project. The company developed a software data processing module enabling real-time data exploitation of the information from unmanned aerial systems, ground radar stations at the main operating base.



TOSHKO PUNCHEV
VP of Defense Solutions at Wiser

"That's where we learned the demands of military software. Security, documentation, coordination. These are practices you can't learn outside a real project."

The team (back then under the Bianor brand) delivered under NATO standards for communication, image, and video processing, a performance that earned them recommendations from Selex ES (now Leonardo). Over time, the company secured a place in eleven EDIDP and EDF projects, with two more now being added — over a dozen defense and space programs to date.

ASTERION: Enabling secure, real-time underwater communication

One of Wiser's most recent and technically complex engagements is ASTERION, a 36-month EDF-funded project focused on building a secure, adaptable underwater communication network using ultrasound and laser signals.

*"The goal is to create a hardware-software prototype for encrypted underwater mesh networking over kilometer-long distances," **Punchev explains**. "It sounds simple on paper, but seawater introduces refraction, interference, and unpredictable signal behavior. We need to detect and mitigate all of that."*

Wiser brings specialized knowledge in ultrasonic protocols, including experience with UDXP, which may soon become an IEEE standard. However, its core value lies in the structure it brings to the entire development process, which is a component often missing from research-heavy consortia.

"We apply MIL-STD-498 across the board – processes, phases, documents," says Punchev. "We maintain a license for IBM DOORS to trace requirements and use Enterprise Architect for software modeling. This gives us a unified approach that defense ministries across the EU expect."

In a consortium of over thirty organizations – many focused on exploratory research — Wiser fills a gap by turning fragmented components into interoperable systems that can meet defense-grade reliability and traceability requirements.

MARTINA: Validating AI for satellite image analysis

Wiser also plays a central role in MARTINA, a 48-month EDF project that focuses on evaluating how reliably AI systems can interpret satellite imagery for defense purposes.

Here, Wiser is not building the AI – it's building the evaluation infrastructure.

The team is responsible for the user identity and access portal, as well as a scalable backend that handles data management, workflow orchestration, and result submission.

Based on prior experience from European Space Agency projects in road safety and infrastructure monitoring, they also contribute to AI lifecycle tooling and help define dataset evaluation frameworks.

According to the company, MARTINA demonstrates how experience from civilian space applications can be transferred to defense, provided the systems are designed for traceability and reuse.

Not just code – systems that hold together

Wiser's work is rarely visible to end users, but it is fundamental to how systems behave in practice.

VENTSISLAV NEYKOV
VP of Technology and Innovation at Wiser

"We aim to be a trusted, end-to-end engineering partner – not just a vendor, our goal is to make systems behave reliably, across components we don't fully control. In these industries, best practices aren't a choice – they're a requirement. Everything passes through validation gates. We test at every level: unit, integration, system."

This thinking also extends to AI projects. In FaRADAI, Wiser contributed object recognition models trained on low-data environments, including systems designed to identify camouflaged tanks in battlefield conditions.

Why partners return: Engineering built for handover

Wiser's reputation has grown not through marketing but through repeated delivery. In some EDF projects, the company has been invited to join consortia based on past collaboration – a signal of trust in both its reliability and its approach.

Crucially, Wiser doesn't build dependency.

"Our goal is to hand over working systems that others can operate and maintain. We document everything. We train internal champions. That's how transformation sticks – not through code, but through ownership," - Neykov says.

Wiser's rise is part of a larger shift: Central and Eastern Europe is no longer just a cost-efficient engineering pool. In programs like ASTERION and MARTINA, Bulgaria is contributing software that underpins core EU defense capabilities.

To meet rising demand, Wiser is expanding its team – but with care.

> *"We're looking for 'three-in-one' people, strong programming fundamentals, experience in multiple domains, and the curiosity to learn defense standards. Education systems aren't producing them, so we train internally."* - ***says Punchev.***

With a team of over 600 and a governance model that ensures independence and continuity, Wiser Technology is becoming a reference point for how CEE companies can deliver long-term value in strategic domains.

NAVIGATING THE DUAL-USE DILEMMA

Navigating the Dual Use: Balancing Innovation with Security

Author: Teodora Atanasova

By mid to late 2023, Ukrainian units repurposed low-cost agricultural drones to launch 15 kg of explosives against Russian armor.[1] Within days, equipment built for crop analysis became an improvised artillery system.

It's not a rare example – the fast deployment of dual-use technologies in response to current challenges is far from uncommon. The stakes are higher than ever, as their use becomes increasingly critical.

Europe's geopolitical environment – marked by Russia's invasion of Ukraine and strategic competition in the Indo-Pacific (in which European countries are indirectly involved) – has driven the commercialization of dual-use technologies. For example, EU member states' authorized dual-use exports were €57.3 billion in 2022, up from €38.5 billion in 2021 – a roughly 49% year-on-year jump.[2]

Crucially, these market shifts run alongside with deep supply-chain realignments that further shrink the interval between prototype demonstration and operational deployment. By improving the integration of R&D, manufacturing, logistics, and digital systems, Europe can shorten time-to-deployment, enabling front-line testing and fielding cycles in weeks or months rather than years under traditional procurement.

What happens then when technologies, initially developed to boost European agriculture are adapted for military use; would they really be efficient? What does history teach us about today's efforts to integrate R&D, manufacturing, logistics, and digital systems for rapid defense deployment?

Over the past century, Europe has often had the "dilemma" to balance the everyday uses of technology with its potential military impact.

Historical growth of dual-use tech in Europe

During World War I, the pioneering Haber–Bosch process, developed by Fritz Haber and Carl Bosch, was originally adopted to produce ammonia for fertilizers but it also became indispensable for munitions, supplying Germany with explosively-active nitrates despite naval blockades. That very duality led to some of the earliest calls for controls on dual-use chemical compounds. After World War II, Western allies established CoCom (1949) to restrict technology transfers to the Soviet bloc.[3] CoCom's export controls covered radar components, semiconductors and nuclear technology.

Building on these wartime-era controls, the European Community formalized its own regulatory mechanisms. In 1994, the European Community introduced Council Regulation 3381/94, requiring authorizations for the export of sensitive dual-use goods. Just two years later, the Wassenaar Arrangement brought over 40 countries together to coordinate controls on arms and emerging technologies.

That concern has only intensified. By 2018, the EU had begun to identify software and biotechnology as increasingly sensitive dual-use domains. To keep pace with new threats, the EU passed Regulation 2021/821, which introduced a more flexible system that allows export restrictions on emerging or high-risk technologies – even if they're not specifically listed. The regulatory shift was not merely bureaucratic; it was a reaction to the rising flow of sensitive tech.

Investment switch

A few years later, bolstered by the war in Ukraine, Europe's innovation economy has become a driving force in the dual-use space. In 2023 alone, the European Investment Fund committed significant resources into dual-use and deep-tech ventures via instruments like a €25 million deep-tech fund in CEE and a €175 million Defence Equity Facility.[4]

In early 2025, the European Defence Fund (EDF) received an additional €1.5 billion under the Strategic Technologies for Europe Platform (STEP) for 2024–2027 to support dual-use and defense R&D.

> The message was clear: in Europe, dual-use innovation is no longer balanced between civilian and military aims – it is tilting firmly toward the defense end of the spectrum. At the same time, private and public investment in this space is still drawing increased scrutiny, as policymakers and investors weigh the ethical and strategic implications of funding technologies with potential combat applications.

European sustainability-focused (ESG) funds have significantly increased their holdings in defense stocks since the war in Ukraine started, which sparked a reassessment of their traditionally strict ethical exclusions. Specifically, exposure to defense among these funds more than doubled – from approximately €3.2 billion in Q1 2022 to around €7.7 billion by Q3 2024, according to Morningstar data cited by the Financial Times.[5–6]

Yet on the ground, the operational shift by companies toward battlefield-specific applications remains limited. While many companies in the region have deployable technologies, relatively few are currently tailoring their operations toward battlefield or defense-specific use. This gap, especially in times of crisis, could prove important to address.

Ambiguity surrounding dual-use technology

This lack of structural support in CEE and, increasingly, across Europe is further complicated by growing uncertainty around what dual use really means.

As the term gains currency in both policy circles and funding programs, its scope is becoming dangerously vague. EU policy frameworks and initiatives like the European Defence Fund (EDF) and Horizon Europe routinely prioritize dual-use potential when awarding grants, but many startups, particularly those working on direct military applications, find the label too broad to be useful in practice.[7]

As Jan-Erik Saarinen, founder and CEO of Double Tap Investments, notes, the ambiguity surrounding dual use can lead to misinterpretation.

"I'm somewhat fatigued by the topic of 'dual use' – it's often misunderstood or misapplied. For example, someone might argue that investing in a pen factory is dual use because a pen can be used at the front. That kind of logic dilutes the real meaning of the term," he explains.

While Saarinen acknowledges that many of the technologies his investment company backs will likely have civilian applications in the long term, his focus remains on impact: "*Our goal is very clear – we are investing in tech that can help end the war as quickly as possible*."

This urgency reflects a broader shift in the perception of defense innovation.[8] For many investors, the line between ethical and unethical is no longer defined by category, but by purpose.

Saarinen observes that just a few years ago, managing large investment portfolios often involved heated debates about the ethical boundaries of sectors like gambling, tobacco, adult content, and defense. However, he notes a noticeable shift in perspective: in today's geopolitical climate, defense is increasingly being reconsidered through the lens of national security and humanitarian responsibility.

Kateryna Bezsudna, co-founder and CEO of Defence Builder, underscores this tension:

"The main worry is keeping critical technologies out of the wrong hands – this is where we start talking about IP protection measures. Sure, regulation can scare off some startups from entering the defense sector, but security has to come first."

To manage these risks without stifling innovation, initiatives like Ukraine's Brave1 cluster and Defence Builder accelerator are offering a path forward. "*There are ways to deal with overregulation*," Bezsudna adds.

"Clusters like Brave1 and growing interest from both international and Ukrainian investors help startups work through regulatory hurdles while keeping security standards intact. It's all about striking that right balance – encouraging innovation while making sure our critical tech stays secure."

Regulatory gaps

But while investment flows into defense-aligned technologies, regulation hasn't kept pace. *"Especially when it comes to critical technologies that Europe needs to acquire quickly in order to achieve strategic autonomy, over-regulation can be a harmful factor that essentially presents a barrier to market access for smaller players and defense startups,"* says Peter Kováč, a specialist in Defense & Security at SAP, who focuses on AI development in the defense sector.

"Such smaller companies can be Europe's competitive advantage over the rest of the world, provided that it can fully harness its innovative potential."

This tension is even more pressing in Central and Eastern Europe, where a new generation of defense-focused startups is emerging from countries like Poland, Romania, and the Czech Republic. Yet despite growing momentum, many of these ventures encounter practical hurdles. Regulatory complexity, evolving legal frameworks, and limited access to defense-focused investment continue to challenge the growth of dual-use startups in the region.…

"Founders here are building serious technology," explains Leos Mauer, Czech NATO DIANA Accelerator Lead. – *"But they're operating in a system that wasn't designed for speed, equity flexibility, or cross-border dual-use growth."*

Not a dilemma anymore

The dual-use dilemma is no longer theoretical. Europe must walk a tightrope between innovation and security. Failing to manage dual-use risks could lead to strategic vulnerabilities; overregulating could stifle the very innovation needed to ensure sovereignty.

Smart, responsive regulation is key. This involves improving export control coordination, providing better support for defense-related startups, and encouraging international collaboration.

Now is the time for Europe to act decisively. The path is complex, but the stakes are too high to ignore.

REFERENCES

1. “China Supplies Drone Components to Russia, U.S. Officials Warn” – The New York Times https://www.nytimes.com/2023/09/30/technology/ukraine-russia-war-drones-china.html
2. “Report Highlights EU’s Strengthened Approach to Controlling Dual-Use Exports: European Commission” – Directorate-General for Trade and Economic Security https://policy.trade.ec.europa.eu/news/report-highlights-eus-approach-export-controls-dual-use-items-2025-01-31_en
3. “Chapter 9 – Statutory and Regulatory Controls: The Export of Our Militarily Sensitive Technology”; U.S. House of Representatives Select Committee Report 105-851, Report of the Select Committee on U.S. National Security and Military/Commercial Concerns with the People’s Republic of China (105th Congress) https://www.govinfo.gov/content/pkg/GPO-CRPT-105hrpt851/html/ch9bod.html
4. “EU Launches €175 Million Defence Equity Facility to Boost Private Investment in Dual-Use Technologies”; European Investment Fund (EIF) – InvestEU Program https://www.eif.org/InvestEU/defence-equity-facility/index.htm
5. “Defence investing booms from war in Ukraine” – PA Europe https://europe.portfolio-adviser.com/defence-investing-booms-from-war-in-ukraine/
6. “ESG investors’ dilemma over bombs and bullets” – Financial Times https://www.ft.com/content/f0bddcc0-2a99-4153-8510-613efc243d9d
7. “White Paper on Dual-Use Technologies: Advancing Innovation Across Civilian and Defence Applications”; European Commission – Directorate-General for Defence Industry and Space (DG DEFIS) https://research-and-innovation.ec.europa.eu/system/files/2024-01/ec_rtd_white-paper-dual-use-potential.pdf
8. “First investment in dual-use defence technologies”; EIF Annual Report 2024 – Financial Times https://www.ft.com/content/860a6f9b-c821-45a5-b893-a6ec38d4d273

From Conflict to Capability: The Next Wave of Strategic Infrastructure Will Be Born in Defense

How Presto Tech Horizons Is Backing Frontier Startups With Insider Access, Cross-Border Scale, and a €150M Bet on Resilience

LUCIE BRESOVA
Partner at Presto Tech Horizons

Over the past five years, the world has been living through a continuous stress test: war on Europe's borders, energy insecurity, a global pandemic, supply chain fragility, and rapid technological escalation. In times like these, innovation accelerates – not just for defense, but for resilience. From GPS to the internet, some of the most transformative technologies of the last century began as military tools. The same could be true today.

Presto Tech Horizons is betting on that future. Backed by venture firm Presto Ventures and industrial group Czechoslovak Group (CSG), the fund aims to invest €150 million in dual-use, defense, and security technologies from NATO countries and allies. Its thesis: investing in resilience is not just about protection – it's about enabling breakthroughs across logistics, manufacturing, energy, healthcare, and beyond.

In this interview, Lucie Bresova, Partner at Presto Tech Horizons, breaks down why Central and Eastern Europe (CEE) can no longer be viewed as one market, how the venture landscape is becoming increasingly specialized, and what types of founders and technologies may define Europe's strategic future.

You argue that CEE can no longer be viewed as a monolithic region, especially in defense innovation. What structural differences between countries like Poland, the Baltics, and the rest of CEE are most decisive for investors today?

Lucie: Yes, I'd push back on the idea of "one CEE market". In defense tech, we actually see three distinct theatres, perhaps four. Poland is the scale play: it's spending nearly 5% of GDP on defense next year and offers huge

offset-driven opportunities for hardware and integration. The Baltics are the speed play: tiny budgets but a digital-first culture,

DIANA (Defence Innovation Accelerator for the North Atlantic) accelerator sites, and the highest startup density in Europe mean that founders can test with frontline units within months.

The rest of CEE is an optionality play, featuring good engineering talent and new initiatives such as the European Defence Fund (EDF) and DIANA hubs. However, procurement and capital markets are still catching up. Ukraine, of course, is in a league of its own.

Given that Presto Tech Horizons focuses on finding top talent globally rather than investing regionally, how do you assess and compare defense tech founders from the US, Israel, Western Europe, and CEE?

We screen founders on a five-axis scorecard: domain insight, tech moat, speed to first contract, capital leverage, and global compliance mindset. Each region has its own specifications, mostly driven by local culture.

Your collaboration with Czechoslovak Group (CSG) signals a shift toward 'competitive VC products' in a maturing market. How do you envision specialized funds reshaping the resilience investment landscape?

We generally think of venture capital along two axes: global versus regional, and generalist versus specialist. That brings us to four distinct groups:

Global generalists like Sequoia, a16z, or SoftBank deploy billion-dollar pools everywhere. They hire defense partners, but resilience is just one of perhaps 20 themes they cover.

Regional generalists back everything in their home markets.

Regional specialists focus on a single sector in a specific country. Such funds exist and perform well in the US, but this model is challenging to implement and somewhat unrealistic in Europe.

Global specialists delve deeply into a narrow set of technologies but operate widely across borders. This model is winning in resilience tech because hardware, export controls, and sovereign buyers demand surgical expertise and global scale. That's where Presto Tech Horizons really plays to its strengths.

It's very difficult to become a Tier 1 global specialist if you don't have a strong value proposition for startups and investors alike. I think there will be a wave of specialization across the VC landscape.

First Presto Tech Horizons investments

vidarSYS	BAVOVNA	BlueQubit	DIFFUSEDRIVE
A portable AI-driven acoustic localization system to detect hostile battlefield attacks and protect strategic assets	*AI-driven navigation system for uncrewed vehicles operating in environments threatened by electronic warfare*	*QSaaS platform bridging quantum algorithms and practical applications in cryptography, pharma, and logistics*	*GenAI platform for realistic, customizable training data to improve vision AI for autonomous systems*

How does this model - with a deep sector focus and cross-border reach - translate into concrete advantages for startups operating in resilience tech?

The partnership between Presto and CSG, one of Europe's fastest-growing primes, is unique in the VC world. Our joint venture model gives startups something rare: the ability to scale with insider access. That includes asymmetric information, a streamlined path to government and commercial customers, and even exit opportunities.

We're not just offering capital to our portfolio companies – we're offering credibility, relationships, and a practical edge that's essential in the defense space. That can be the difference between securing a first contract or being stuck in an endless pilot loop.

On the other side of the coin, how do we involve more investors in defense and resilience tech?

Defense and security industries come with high entry barriers. Most investors don't have the time or positioning to maintain a regular presence at specialized industry events, limiting their access to high-quality deal flow.

Without visibility and insider contacts, it's difficult to uncover a strong pipeline of relevant startups. And even when they do, evaluating them is another challenge. Navigating regulatory and compliance requirements, especially for dual-use technologies, is complex. Investors rarely have the expert networks they'd need to assess technical and commercial viability in areas like satellite communications or advanced biotech.

Presto Tech Horizons was designed to help investors overcome these structural barriers. Through our partnership with CSG, we provide sector expertise, insider networks, and market access that most investors can't build on their own. Deep tech in this space also tends to be capital-intensive. Early monetization and go-to-market require more than funding, you need infrastructure and processes. We combine financial resources with industry know-how and build a viable path for investors and entrepreneurs to operate effectively in this highly specialized domain.

What are some specific examples of resilience technologies that signal the direction of the sector?

It's easy to associate defense tech with drones and armored vehicles. But resilience innovation is much broader, and increasingly applicable across civil domains.

Consider thermal satellite imaging, which supports both national security operations and environmental monitoring. Or industrial laser systems, essential for advanced manufacturing in aerospace and defense but also shipbuilding, for example.

Other technologies include visual navigation systems that enable autonomous movement in GPS-denied environments, acoustic wave systems that keep optical surfaces clear in harsh conditions, and AI tools for anomaly detection and prompt injection protection.

Each of these solutions addresses strategic challenges, but their impact extends far beyond the battlefield.

Where do you see the strongest overlaps between civilian space technologies and defense applications, and how important will dual-use potential be for future investments?

Space tech is a great example of a dual-use technology with many use cases. To highlight a few, I'd mention data from orbit, secure connectivity, and on-orbit manoeuvre and safety. Wherever those layers intersect, the same hardware can earn a civil invoice on Monday and a defense invoice on Friday.

Another important driver: AI. Really the key element underpinning much of the future defense and resilience tech. We see it in most of the startups we meet and assess. And as an institutional investor, we're focused on backing projects that will strengthen European resilience and tech sovereignty well beyond the end of the war in Ukraine.

MAPPING CEE COMPANIES

Methodology

This report, “Who Is Protecting Europe’s Future”, is a strategic mapping of innovation in the defense technology and cybersecurity sectors across 19 countries in Central and Eastern Europe (CEE).

Our goal was not only to quantify and categorize innovation across these emerging ecosystems, but also to understand how regional players contribute to Europe’s collective ability to defend itself in increasingly volatile times.

That is why beyond raw mapping, this report weaves in editorial themes to capture the human, strategic, and geopolitical dimensions of innovation.

Research approach

We combined desk research with qualitative interviews, engaging with dozens of domain experts from both defense/dual-use and cybersecurity sectors. This dual approach allowed us to zoom in on granular developments – like startup performance and sector specialization – while zooming out to capture macro trends through editorial storytelling across the report.

Our primary tool for company-level insights was **Dealigence**, an intelligence platform focused on real-time visibility into private markets. Unlike most platforms that rely on static, public data, Dealigence tracks more dynamic performance signals – such as headcount trends, product adoption, recurring revenue growth, and even unannounced funding rounds – giving us a more accurate and up-to-date view of how startups are truly performing.

In addition, we cross-verified all findings using well-known databases such as Dealroom, Crunchbase, and PitchBook, and consulted local ecosystem mappings, investor reports, and government registries wherever available.

Selection Criteria

We intentionally focused on active and innovation-driven players – primarily startups, scaleups, product companies, and spin-offs – operating in defense/dual-use and cybersecurity sectors.

Given the nature of early-stage ecosystems, we acknowledge there will never be a definitive count of players. However, we made a conscious effort to include only those teams with visible traction, clear specialization, and current activity in the market.

There are a few important caveats to note:…

In the **Ukrainian defense tech** ecosystem, the situation is highly fluid. Some claim there are hundreds of startups forming under wartime conditions. For the purpose of consistency and accuracy, we adopted a **reserved stance**, including only teams with verifiable traction or notable visibility.

In **cybersecurity**, the services segment – while highly active – was not the focus of this research. We concentrated instead on teams building new products, even if they are not traditional startups (e.g. product-focused vendors or spin-offs).

Across all countries, **company inclusion was based on observed activity.** Despite best efforts, some early-stage or stealth companies may have been missed due to lack of public information. For these reasons, startup numbers per country should be viewed as estimates, not absolutes.

Dual-Use Context

Given the ambiguity surrounding the term “dual use” – as many technologies can be adapted for military or civil security use – we concentrated on companies that show not only technical potential but also strategic intent to engage defense-related markets. This included clear signals such as:

- Defense-oriented product positioning;
- Integration readiness for battlefield or security applications;
- Demonstrated interest in public procurement, R&D partnerships, or strategic defense collaborations.

While many CEE tech companies have deployable capabilities, only a subset are currently structuring their business and product strategies around defense needs. Bridging this intent-to-application gap remains one of the most critical challenges for Europe's innovation pipeline in defense.

To identify these players, we again relied on Dealigence for signal-based analysis, and cross-referenced our findings with other commercial and government databases to ensure a comprehensive and credible mapping.

Talent Mapping

One of the recurring challenges across the CEE region is mapping the actual size and depth of the talent pool in cybersecurity and defense tech. A comprehensive view of sector-wide human capital is difficult to achieve using public data alone – especially given that platforms like LinkedIn offer limited visibility, suffer from self-reporting inconsistencies, and often underrepresent freelance, contract, or military-affiliated specialists.

For this report, we relied on Dealigence's proprietary filtering system to estimate the number of full-time employees in each mapped company. This system is designed to surface only valid, full-time team members and removes profiles based on the following signals:

- Obvious bots or fake-looking accounts;
- Missing or vague experience details;
- Stakeholders like investors, advisors, or board members;
- Irrelevant job titles (e.g., "chef", "bartender");
- Freelancers, students, part-timers, or contractors.

What remains is a high-integrity headcount – our best approximation of actual full-time staff per company. As such, while the numbers presented reflect startup and scaleup team sizes, they do not represent the full defense-tech and cyber talent pool in each country.

Data Points and Structure

Each country profile follows a standardized format, including:

Quantitative data: Number of startups/product companies, total funding those companies received over their lifetime, top investments for the 3 year period (April 2022 – April 2025) in each sector, and most active investors (the ones that had the most recurring investments in that country, for that sector; including ecosystem facts such as defense budgets and sector-focused education.

Qualitative insights: Focus areas (most prominent specializations of mapped companies), key players and startups to watch (assessed by their venture maturity and potential), including ecosystem support mechanisms such as cyber strategies and international partnerships.

To ensure consistent financial reporting across regions, **all funding figures were converted to euros** using a flat exchange rate of **$1 = €0.88**. This helped normalize the data across currencies and sources.

Additionally, instead of focusing on a single calendar year, we used a **rolling three-year investment window (April 2022 – April 2025)** for funding analysis. This decision was made due to uneven investment activity across many ecosystems; in some countries, a single year (e.g., 2024) would not yield a representative picture of innovation trends or capital deployment

By combining data intelligence with expert insight and contextual storytelling, we hope this report provides a compelling, multi-dimensional view of the innovation forces shaping Europe's defense future from its CEE frontier.

If there are any discrepancies and errors you have noticed, or if you want to consult us about our research, please let us know over email newsroom@therecursive.com.

CEE Overview: Defense & Dual Use

Companies

There are 170+ defense/dual-use startups in the CEE region.

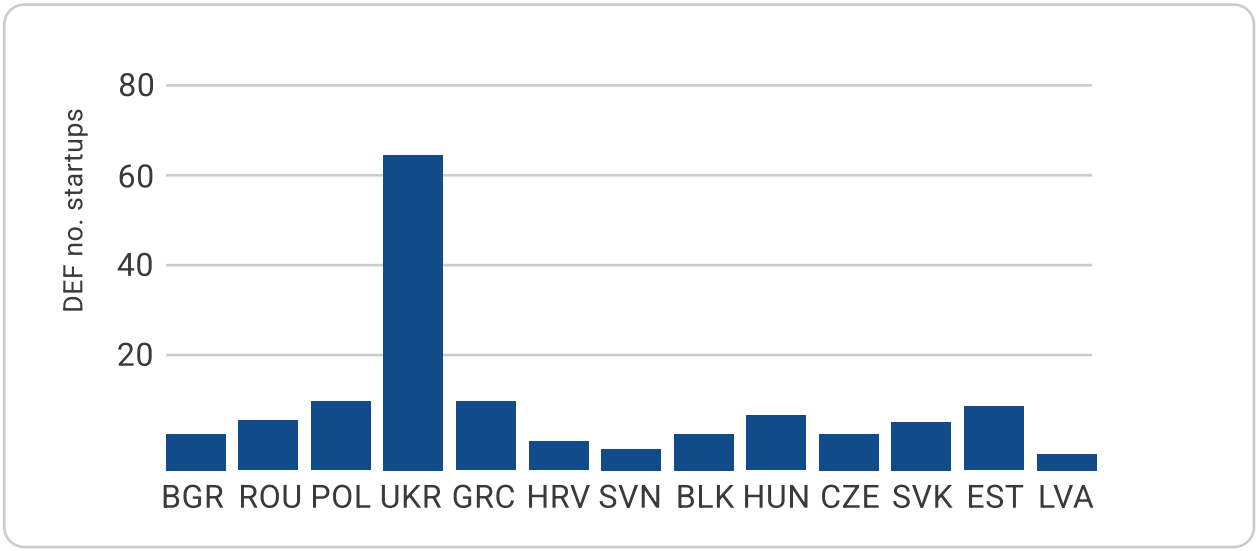


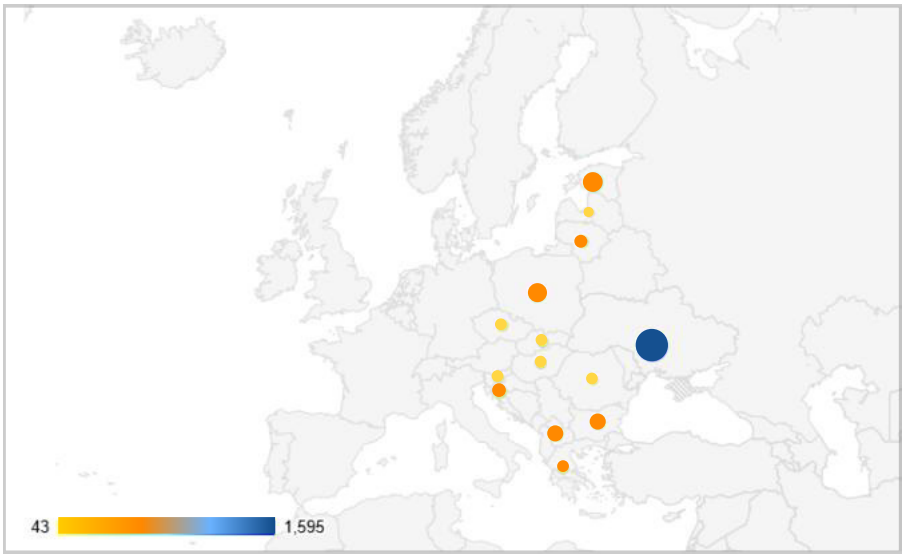
Table 1 - Number of defense or dual-use companies per country

Their dominant focus areas are:

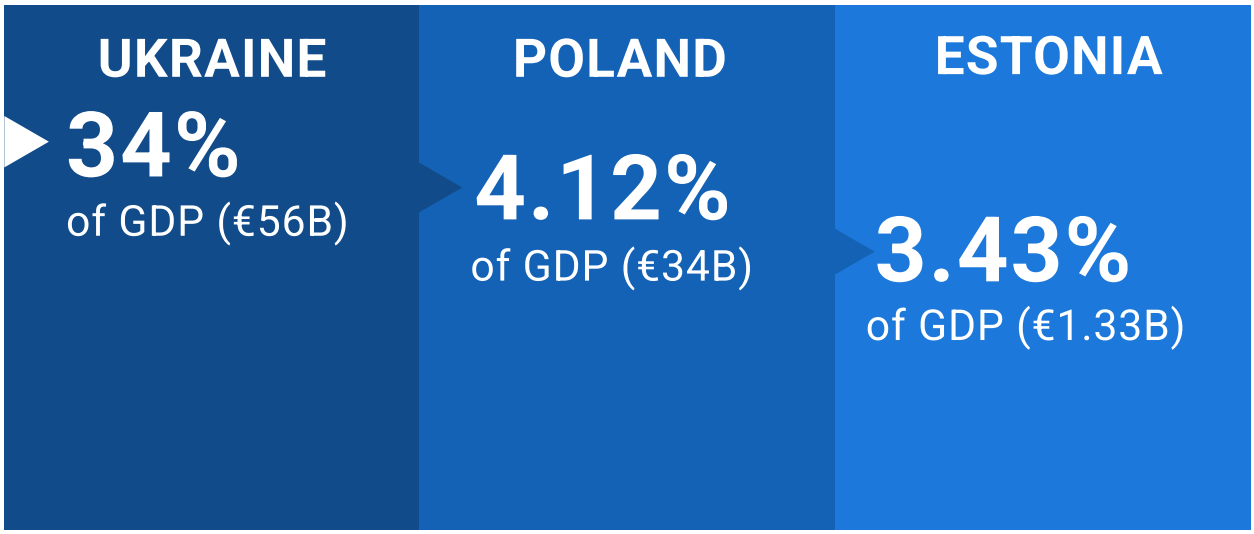
- Autonomous Systems
- AI & Machine Learning
- Drone / UAS / UAV
- Robotics

Talents

Those companies employ 4,000+ full-time employees.



Top 3 countries with the highest defense budget in 2024 as per % of GDP:



Top 5 countries by the number of military academies offering tech or cybersec related programs:

1. Poland (5)
2. Greece (4)
3. Romania (4)
4. Bulgaria (2)
5. Balkans (6)

Funding

Total funding those companies received

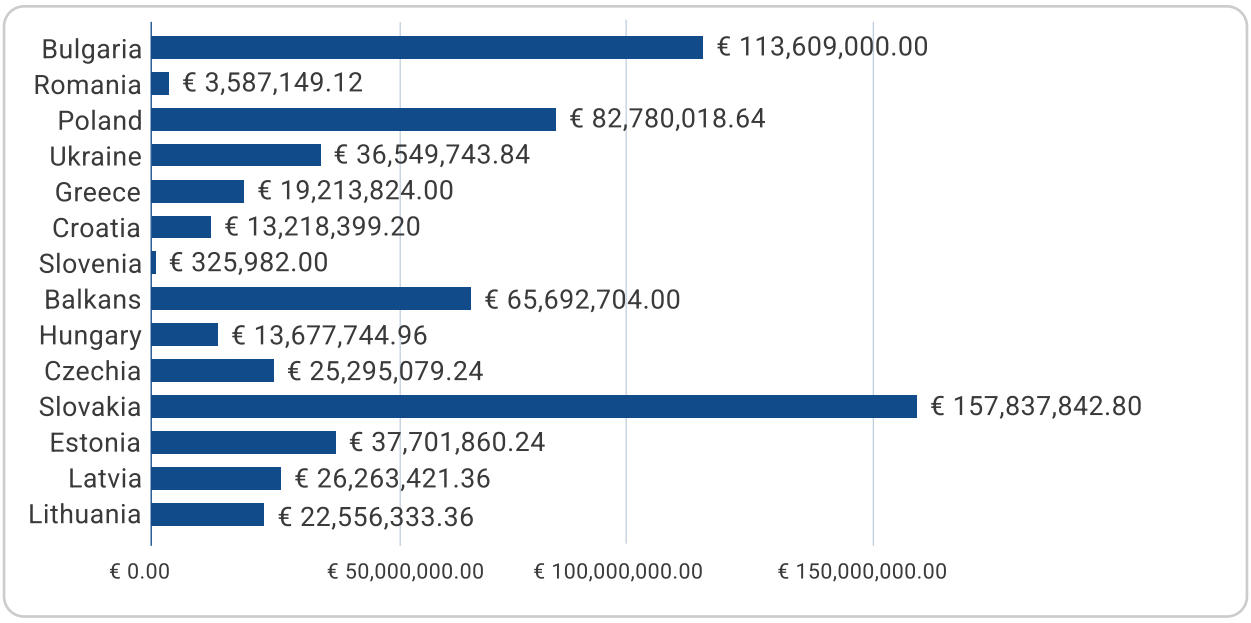


Table 2 - Defense tech & dual-use total funding vs. Country

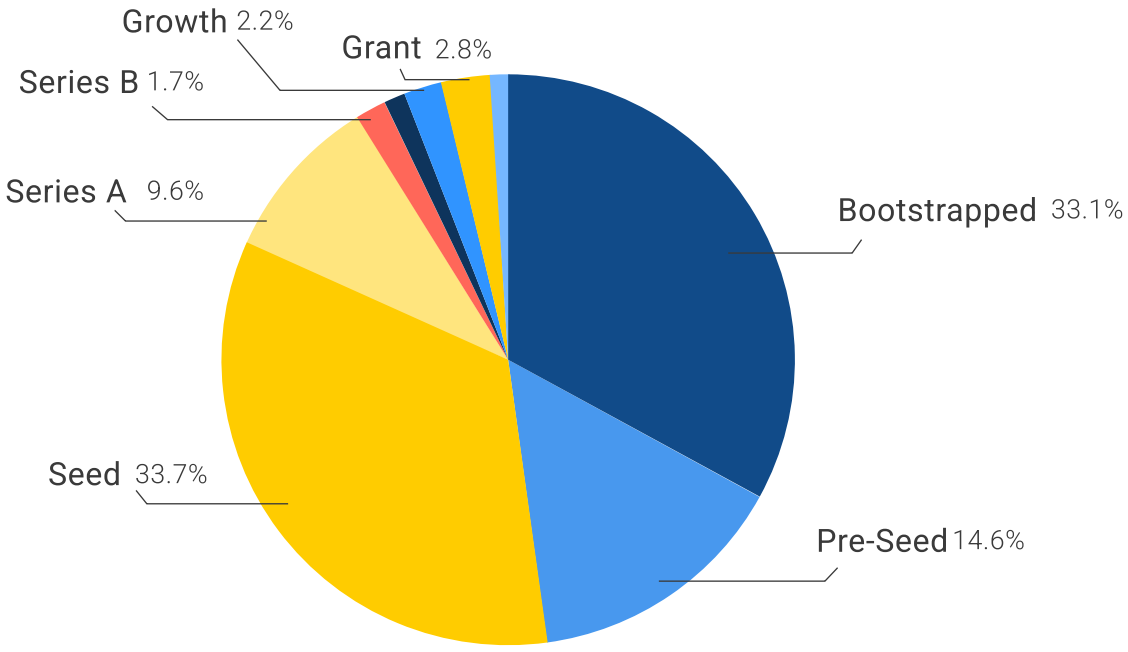
10 the most funded defense/dual-use companies in the region:

1. InoBat
2. Dronamics
3. EnduroSat
4. Liftero
5. CloudFerro
6. Thorium Space Technology
7. Picogrid
8. Vrgineers
9. Orqa FPV
10. Delian Alliance Industries

Most active investors in the sector:

1. SMRK VC
2. Nezlamni Fund
3. ESA BIC Estonia
4. ESA BIC Czech Republic
5. CzechInvest

Investment round distribution.



Top 5 investments (April 2024 - April 2025)

1. **InoBat** /Series C/ €100M
2. **EnduroSat** /Capital raise/ €20M
3. **Picogrid** /Seed/ €10.56M
4. **Dronamics** /Grant/ €10M
5. **Orqa FPV** /Seed/ €5.8M

CEE Overview: Cybersecurity

Companies

There are 280+ cybersecurity startups and product companies in the CEE region.

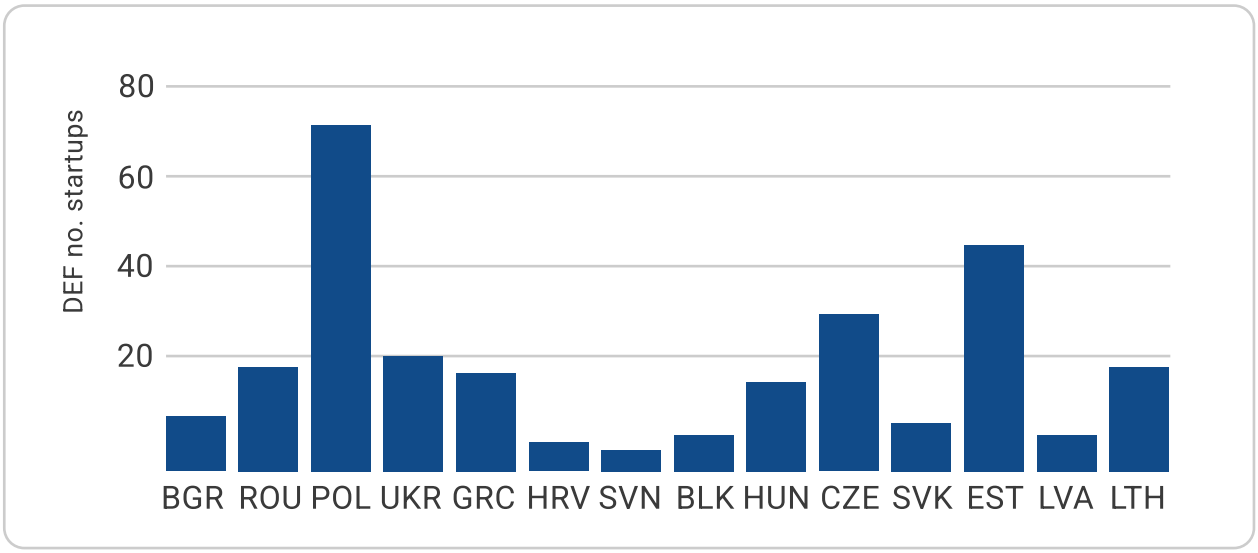


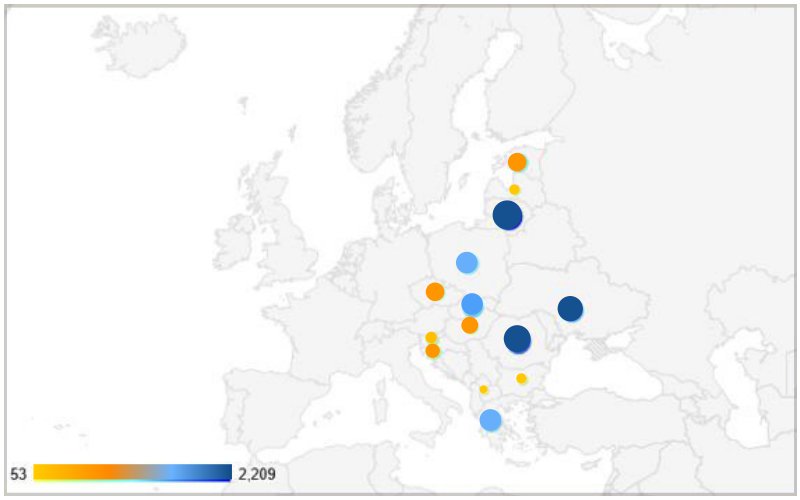
Table 1 - Number of cybersecurity startups and product companies

Their dominant focus areas are:

- Identity and Access Management (IAM)
- Security Operations & Threat Management
- AI & Machine Learning-Driven Cybersecurity
- Data Privacy & Encryption

Talents

Those companies employ 12,000+ full-time employees.



Graphic 1 - Distibution of full-time employees per CEE country

Biggest employers in the region are:

Bitdefender	ESET	Nord Security
1010 full-time employees in CEE	973 full-time employees in CEE	877 full-time employees in CEE
Romania	Slovakia	Lithuania

Top 5 countries by the number of universities offering cybersecurity-related programs:

1. Ukraine (41)
2. Poland (29)
3. Greece (28)
4. Romania (28)
5. Czechia (20)

Funding

Total funding those companies received:

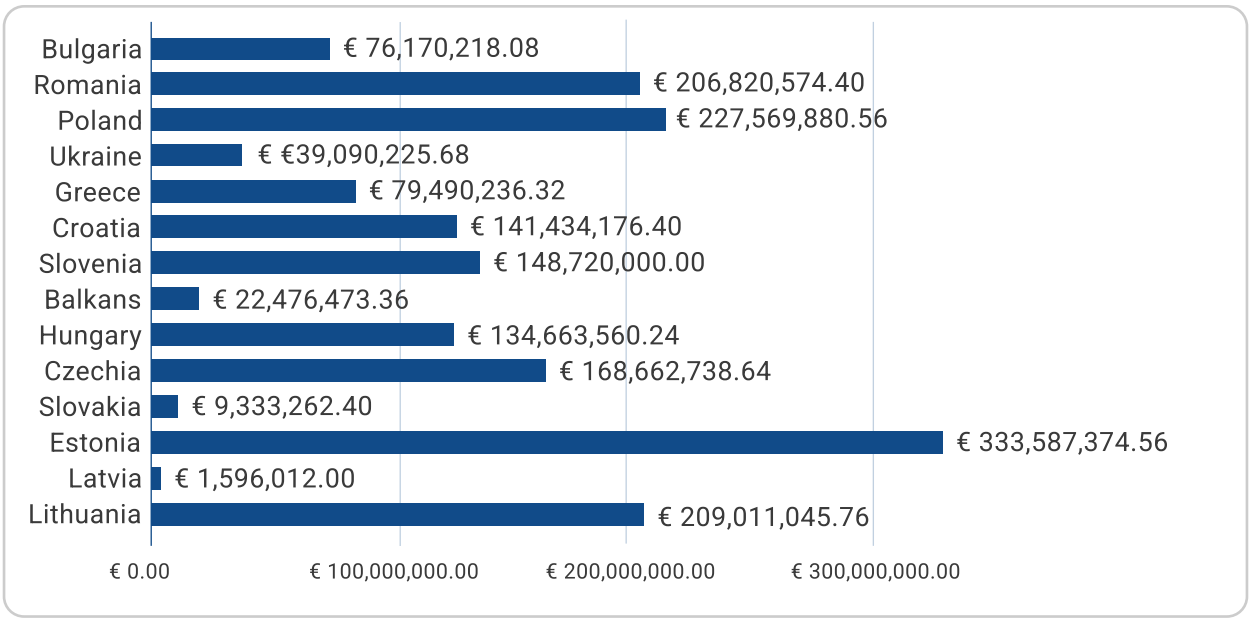


Table 2 - CYB total funding vs. Country

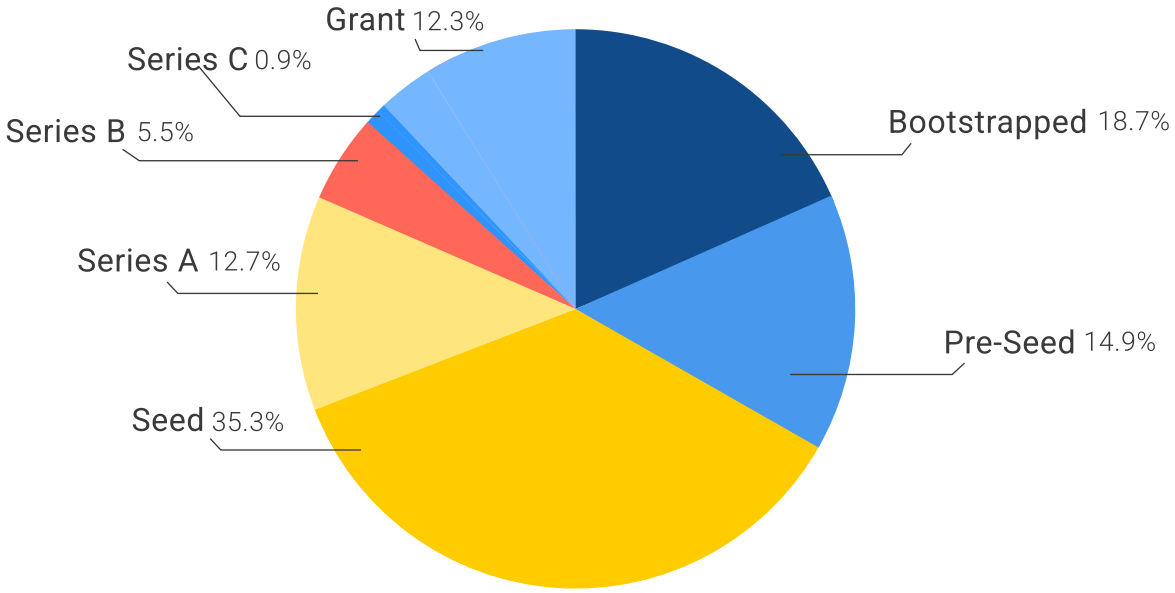
10 the most funded cybersecurity companies in the region:

1. Nord Security
2. Bitdefender
3. Veriff
4. HYCU, Inc.
5. SEON
6. Reversing Labs
7. Hack The Box
8. Alcatraz AI
9. Blackwall (formerly BotGuard OÜ)
10. Microblink

Most active investors in the sector:

1. Startup Wise Guys
2. Credo Ventures
3. Space3ac
4. Presto Ventures
5. Hiventures

Investment round distribution.



Top 5 investments (April 2024 - April 2025)

1. **Blackwall** /Series B/ €45M
2. **ThreatMark** /Series A/ €20.24M
3. **Whalebone** /Series B/ €13.35M
4. **E2B** /Seed/ €10.12M
5. **Fudo Security** /Series A/ €8.80M

UKRAINE

DEFENSE/DUAL-USE SECTOR	CYBERSECURITY SECTOR

STARTUPS

65	18

FOCUS AREAS

- Drone Technology & Unmanned Aerial Systems
- Electronic Warfare & Counter-Drone Systems
- Robotics & Unmanned Ground Vehicles (UGV)

- AI-Driven Threat Intelligence & Detection
- Identity & Access Management (IAM)
- Blockchain & Web3 Cybersecurity

TOTAL FUNDING

TOP 3 INVESTMENTS (APR 2022 - APR 2025)

01 Esper Bionics - €4.40M (2024)
02 Osavul - €2.64M (2024)
03 Swarmer - €2.33M (2024)

01 SpinAI - €14.52M (2022)
02 LetsData - €1.55M (2025)
03 Hackless - €1.06M (2023)

MOST ACTIVE INVESTORS

Nezlamni Fund & SMRK VC	Ukrainian Startup Fund

IMPORTANT PLAYERS

	Founded	Stage	Funding	Specialization
Bavovna AI	2024	Seed	€2.38M	Offers AI-driven alternative navigation solutions for unmanned vehicles in GPS-denied and electronic warfare environments
Swarmer	2023	Seed	€2.49M	Develops AI-based software that enables coordinated drone operations with minimal human intervention
HIMERA	2023	Seed	€594K	Universal communication systems resistant to electronic warfare thanks to FHSS technology

2024 Defense Budget: ~ €56 billion (34% of GDP)
Key international ties/partnerships:
NATO Enhanced Opportunities Partner, U.S., UK, and EU bilateral military assistance, Lublin Triangle, Ukraine Defense Contact Group (Ramstein format), Black Sea regional partnerships
Education: 1 national military university with cyber/tech curricula

*Ukraine is **not a NATO member**, but has been a **NATO partner country** since 1991 and participates in NATO's Partnership for Peace and the Enhanced Opportunities Program*

SPIN.AI

Founded: 2017 **Stage:** Series A

Specialization: Security solutions for mission-critical SaaS applications, including risk assessment, backup, and ransomware protection, utilizing advanced AI and ML technologies.

Team size (full time): 57 **Funding:** €14.52M

Investors: Martal Capital, AVentures Capital, Blu Ventures, Silicon Valley Syndicate Club, Blueprint Equity, Unpopular Ventures, Enerdigm Ventures, Transform VC, Santa Barbara Venture Partners (SBVP), Network.VC, Spring Ventures, Nika Tech Family

Clients: Over 1,500 organizations in 100+ countries — including enterprises, SMEs, universities, government bodies; trusted by Google, Vimeo, Domino's, etc.

Startups to Watch: Scalarr, Mantis Analytics, LetsData

National Cybersecurity Strategy: Cyber-Security Strategy of Ukraine 2021
National CERT: CERT-UA
Education: 41+ universities offering cybersecurity-related programs

BULGARIA

DEFENSE/DUAL-USE SECTOR	CYBERSECURITY SECTOR

STARTUPS

7	8

FOCUS AREAS

• Unmanned Aerial Systems (UAS) • Surveillance and Recon • AI and Advanced Sensing	• Identity and Access Management (IAM) • Threat Detection and Response • Secure Cloud Services and Data Protection

TOTAL FUNDING

TOP 3 INVESTMENTS (APR 2022 - APR 2025)

01 Endurosat - €20M (2025) **02** Dronamics - €10M (2024) **03** Bronia AI - €500K (2024)	**01** Alcatraz AI - €22M (2022) **02** Evrotrust - €3.3M (2024) **03** Kikimora - €993K (2023)

MOST ACTIVE INVESTORS

Eleven Ventures	Silverline Capital & Vitosha Venture Partners

IMPORTANT PLAYERS

	Founded	Stage	Funding	Specialization
EnduroSat	2015	Series B	€68M	"Satellite-as-a-Service" solutions to simplify access to space data
Dronamics	2014	Pre-Series A	€66M	Cargo Drone Logistics & Unmanned Aerial Systems (UAS)
Bronia AI	2024	Seed	€476K	AI-powered acoustic signal processing for security and industrial applications

2024 Defense Budget: ~ €2.02B (2.1% of GDP)

Key international ties/partnerships:
PESCO, EU CSDP, SEEDC, Black Sea Defense Cooperation

Education: 4 military academies with tech-innovation curricula

ALCATRAZ AI

Founded: 2016 **Stage:** Series B

Specialization: Uses real-time 3D facial mapping and deep neural networks to automatically enroll an individual based on any current access control method.

Team size (full time): 60 **Funding:** €22.2M

Investors: Almaz Capital, Bossa Invest, Golden Seeds, JCI Ventures, LDV Partners, SeedBlink, Silverline Capital, Mucker Capital, Hemi Ventures, Ruvento

Clients: From Healthcare and Government Organizations to Sports Venues and Telecommunications

Startups to Watch: Evrotrust, Kikimora, Plainsea

National Cybersecurity Strategy: Bulgaria's primary cybersecurity legislation is the Cybersecurity Act, adopted in 2018 to implement the EU Network and Information Security (NIS) Directive.

National CERT: CSIRT.bg

Education: 18+ universities offering cybersecurity-related programs

ROMANIA

DEFENSE/DUAL-USE SECTOR	CYBERSECURITY SECTOR
STARTUPS	
10	19
FOCUS AREAS	
• Artificial Intelligence (AI) & Automation • Aerospace / New Space • Drone & Autonomous Systems	• Threat Detection, Prevention & Response • AI & Machine Learning-Driven Cybersecurity • Data Privacy, Identity & Access Management
TOTAL FUNDING	
	
TOP 3 INVESTMENTS (APR 2022 - APR 2025)	
01 OxidOS Automotive - €1.1M (2022) **02** Orbotix - €500K (2023) **03** Grayscale AI - €96K (2023)	**01** Arcanna.ai - €3.1M (2023) **02** Blackshell - €3M (2023) **03** Cyscale - €3M (2022)
MOST ACTIVE INVESTORS	
Innovx - BCR	GapMinder Venture Partners & Early Game Ventures

IMPORTANT PLAYERS

	Founded	Stage	Funding	Specialization
ORBOTIX	2013	Seed	€467K	Autonomous drone systems and advanced robotics tailored for defense and security applications
uRADmonitor	2015	Seed	€29K	Develops and manufactures advanced environmental monitoring devices; primarily operates in the civilian environmental health sector, the underlying tech has direct applicability in defense, homeland security, and disaster response
Skyline Drones	2019	Seed	€392K	Provider of drone based solar panel inspection services

BITDEFENDER

Founded: 2001 **Stage:** Late VC

Specialization: Broad range of IT security products and services that encompass antivirus protection, endpoint security, identity protection, VPN services, and more.

Team size (full time): 1.369 **Funding:** €170.6M

Investors: Vetruvian Partners, Romanian-American Enterprise Fund

Clients: Government organizations, large enterprises, small and medium-sized enterprises (SMEs), and private individuals

2024 Defense Budget: ~ €8.6 billion (2.25% of GDP)

Key international ties/partnerships:
EU CSDP, PESCO, Black Sea Defense Cooperation, Bilateral U.S. defense cooperation (EDI/FMFP), Three Seas Initiative

Education: 4 national military academies/schools with tech/cyber curricula

Startups to Watch: Arcanna.AI, Blackshell, TypingDNA

National Cybersecurity Strategy: Romania's last Cybersecurity Strategy was published in 2021 for the period 2022–2027 + Cyber-Security & Defence Law 58/2023

National CERT: The Romanian National Computer Security Incident Response Team (CERT-RO)

Education: 28+ universities offering cybersecurity-related programs

HUNGARY

DEFENSE/DUAL-USE SECTOR	CYBERSECURITY SECTOR

STARTUPS

11	16

FOCUS AREAS

- Space and Satellite technologies
- Drone and Anti-drone Systems
- Advanced Surveillance Technologies

- Identity and Access Management (IAM)
- Vulnerability and Threat Management
- Data and Infrastructure Security

TOTAL FUNDING

TOP 3 INVESTMENTS (APR 2022 - APR 2025)

01 Perciv AI - €2.5M (2024)
02 Kodesage - €2.3M (2025)
03 N/A

01 SEON - €84.71M (2022)
02 Axoflow - €6.16M (2025)
03 Riptides - €2.90M (2025)

MOST ACTIVE INVESTORS

No recurring investors	Hiventures

IMPORTANT PLAYERS

	Founded	Stage	Funding	Specialization
DiffuseDrive	2023	Seed	€7.92M	An end-to-end automated data solution developed to aid computer vision developers in creating autonomous machines
Kodesage	2024	Pre-Seed	€2.11M	An enterprise-ready solution helping engineering teams modernize complex legacy systems
Perciv AI	2022	Seed	€2.88M	AI-based perception solutions for multiple fields

2024 Defense Budget: ~ €4.38 billion (2.11% of GDP)
Key international ties/partnerships:
EU CSDP, PESCO, Visegrád Group, Defense cooperation with Turkey and Israel, Bilateral U.S. partnership (selective)
Education: 1 national military academy (National University of Public Service) with cyber/tech curricula.

SEON

Founded: 2017 **Stage:** Series B

Specialization: Fraud prevention and risk scoring using digital footprint analysis, machine learning, and data enrichment APIs.

Team size (full time): 270 **Funding:** €101.8M

Investors: IVP, Creandum, Crew Capital, PortfoLion, Discovery Ventures, Fiedler Capital

Clients: 5,000+ clients globally including Miele, Revolut, Nubank, Patreon, and Morning Brew

Startups to Watch: Axoflow, Riptides, BugProve

National Cybersecurity Strategy: New National Cyber-Security Strategy adopted Apr 2025.
National CERT: GovCERT-HU / NCSC
Education: 17+ universities offering cybersecurity-related programs

POLAND

DEFENSE/DUAL-USE SECTOR	CYBERSECURITY SECTOR

STARTUPS

14	71

FOCUS AREAS

• Aerospace & Defense • AI & Autonomous Systems • Sensing & Communications Hardware	• Identity and Access Management (IAM) • AI-Driven Threat Detection & Deception • Blockchain and Cryptography-Based Security

TOTAL FUNDING

TOP 3 INVESTMENTS (APR 2022 - APR 2025)

01 Aleet - €1.14M (2024) **02** SATIM - €1.37M (2024) **03** Liftero - €1.32M (2023)	**01** Fudo Security - €8.80M (2025) **02** Autenti - €8.54M (2022) **03** Authologic - €7.22M (2024)

MOST ACTIVE INVESTORS

Hard2beat & Space3ac	Space3ac & Satus Starter VC

IMPORTANT PLAYERS

	Founded	Stage	Funding	Specialization
Aleet	2018	Seed	€1.40M	AI-powered fleet management platform for route optimization
Thorium Space Technology	2017	Series A	€12.24M	Next-generation satellite platforms and communication payloads, particularly advanced DBF transponders
Advanced Protection Systems Inc.	2015	Seed	€1.37M	A system for detecting and neutralizing drones, capable of reliable operation in various weather conditions and across significant distances

FUDO SECURITY

Founded: 2012 **Stage:** Series A

Specialization: Privileged-Access Management (PAM) platform with real-time session monitoring, zero-trust controls and AI-driven insider-threat detection.

Team size (full time): 70 **Funding:** €9M

Investors: bValue Growth Fund, early angel founders (Patryk Brożek & Paweł Dawidek)

Clients: ~500 organisations in 35 countries across finance, energy, telecom, transport and public sector

2024 Defense Budget: ~ €34 billion (4.12% of GDP)

Key international ties/partnerships:

EU CSDP, PESCO, Visegrád Group, Bilateral U.S. defense agreements (permanent troop presence), Lublin Triangle (with Ukraine and Lithuania)

Education: 5 national military academies/schools with tech/cyber curricula

Startups to Watch: Vidoc Security Lab, Secfense, ResQuant

National Cybersecurity Strategy: Cyber-Security Strategy of the Republic of Poland 2019-2024 (update for 2025-30 in consultation).

National CERT: CERT Polska (NASK)

Education: 29+ universities offering cybersecurity-related programs

GREECE

DEFENSE/DUAL-USE SECTOR	CYBERSECURITY SECTOR

STARTUPS

9	17

FOCUS AREAS

- Autonomous Systems & AI for Defense
- Geospatial & Remote Sensing Solutions
- Underwater Intelligence Systems

- Secure Software Development & VulnerabilityManagement
- Identity & Access Management (IAM)
- Data & Cloud Security

TOTAL FUNDING

TOP 3 INVESTMENTS (APR 2022 - APR 2025)

01 Delian Alliance Industries - €5.58M (2023)
02 Velos Rotos - €1.75M (2023)
03 SOTIRIA Technology - €97K (2023)

01 Hack The Box - €61.60M (2023)
02 PlugSecure - €690K (2025)
03 N/A

MOST ACTIVE INVESTORS

Marathon Venture Capital	Marathon Venture Capital

IMPORTANT PLAYERS

	Founded	Stage	Funding	Specialization
Delian Alliance Industries	2021	Seed	€6.53M	Autonomous systems that integrate advanced robotics, sensors, and proprietary autonomy software to address physical threats rapidly
SOTIRIA Technology	2021	Early-Stage	€88K	Underwater intelligence systems for defense and national security applications
DeepSea Technologies	2017	Series B	€8.10M	Utilizes artificial intelligence to enhance the efficiency of vessels and voyages in the shipping industry

HACK THE BOX

Founded: 2017 **Stage:** Series B

Specialization: Cybersecurity upskilling, threat prevention, detection, and response through gamified training platforms

Team size (full time): 1013 **Funding:** €61.16M

Investors: The Carlyle Group, Paladin Capital Group, Marathon Venture Capital

Clients: Individuals, SMEs, Enterprises, Government Organizations, and Universities

2024 Defense Budget: ~ €7.12 billion (3.2% of GDP)

Key international ties/partnerships:

EU CSDP, PESCO, MED9, strategic partnerships with the U.S., France, and Israel, Eastern Mediterranean trilateral formats

Education: 4 national-level military academies with tech/cyber curricula

Startups to Watch: Futurae Technologies, Bespot, PlugSecure

National Cybersecurity Strategy: National Cyber-Security Strategy 2020-2025

National CERT: National CSIRT-GR under the National Intelligence Service

Education: 28+ universities offering cybersecurity-related programs

CROATIA

DEFENSE/DUAL-USE SECTOR	CYBERSECURITY SECTOR
STARTUPS	
6	6
FOCUS AREAS	
• Autonomous & Robotic Systems • IoT & Connected Platforms • Aerospace & Mobility	• Security Operations & Threat Intelligence • AI Security & Trust for LLMs and Chatbots • Privacy & Data Protection (RegTech)
TOTAL FUNDING	
€13.22M	€141.43M
TOP 3 INVESTMENTS (APR 2022 - APR 2025)	
01 Orqa FPV - €5.8M (2024) **02** N/A **03** N/A	**01** SplxAI - €6.16M (2024) **02** Legit - €650K (2024) **03** N/A
MOST ACTIVE INVESTORS	
No recurring investors	No recurring investors

IMPORTANT PLAYERS

ORQA FPV

Founded: 2018 **Stage:** Seed

Specialization: Develops innovative drone technology aimed at addressing challenges in the FPV (First Person View) market, facilitating remote reality applications

Team size: 77 **Funding:** €7.18M

Investors: Day One Capital, Lightspeed Venture Partners, Decisive Point, Radius Capital

Startup to Watch: Vegvisir (Estonian-Croatian)

Founded: 2021
Funding: €1.2M
Specialization: 360° situational awareness in vehicles & UGVs

2024 Defense Budget: ~ €1.51 billion (1.81% of GDP)

Key international ties/partnerships:
EU CSDP, PESCO, Adriatic Charter, U.S.-Croatia bilateral cooperation, Balkan regional defense cooperation

Education: 1 military academy with tech-innovation curricula

REVERSING LABS

Founded: 2009 **Stage:** Series B/Growth

Specialization: Software-supply-chain security, advanced file & binary analysis, and high-fidelity threat-intelligence services

Team size (full time): 250+ **Funding:** €80.1M

Investors: Crosspoint Capital Partners, ForgePoint Capital, Prelude (Mercato Partners), In-Q-Tel.

Clients: Customers include The Big Tech software companies, top defense & aerospace firms, and multiple Fortune 500 enterprises worldwide

Startup to Watch: SplxAI

Founded: 2023
Funding: €7.87M
Specialization: Cybersecurity solutions for AI applications and chatbots

National Cybersecurity Strategy: Cyber-Security Strategy of the Republic of Croatia adopted in 2015

National CERT: CERT.hr (part of CARNET)

Education: 7+ universities offering cybersecurity-related programs

SLOVENIA

DEFENSE/DUAL-USE SECTOR	CYBERSECURITY SECTOR

STARTUPS

4	5

FOCUS AREAS

• Defense & Tactical Systems • Simulation & Training Tech • Autonomous Platforms	• Data Protection & Encryption • Identity and Access Management (IAM) • Blockchain-Based Trust & Data Integrity

TOTAL FUNDING

TOP 3 INVESTMENTS (APR 2022 - APR 2025)

No disclosed investments	**01** HYCU - Series B Undisclosed (2022) **02** OriginTrail - Seed Undisclosed (2022) **03** N/A

MOST ACTIVE INVESTORS

No recurring investors	No recurring investors

IMPORTANT PLAYERS

GUARDIARIS

Founded: 2007 **Stage:** Growth

Specialization: Custom training solutions for the defense industry, offering advanced simulation software that creates realistic environments

Team size: 125+ **Funding:** Not publicly disclosed

Clients: 15 OEM (Original Equipment Manufacturer) and government clients across Europe, Asia, Africa, and South America

Startup to Watch: C-Astral Aerospace

Founded: 2005
Funding: Bootstrapped
Specialization: Small unmanned aerial systems (UAS/UAV) and services

2024 Defense Budget: ~ €880M (1.35% of GDP)

Key international ties/partnerships:
EU CSDP, PESCO, Adriatic Charter, Bilateral cooperation with Austria and Italy, Balkan regional initiatives

Education: 1 national military academy with tech/ innovation curricula

HYCU

Founded: 2018 **Stage:** Series B/Growth

Specialization: Multi-cloud and SaaS data-protection-as-a-service (DPaaS) for on-prem, public-cloud and SaaS workloads

Team size (full time): 220+ **Funding:** €123.64M

Investors: Acrew Capital, Bain Capital Ventures, Atlassian Ventures, Cisco Investments, Okta Ventures

Clients: 4,200 + organisations in 78 + countries, spanning mid-market to Global 2000 enterprises

Startup to Watch: GlobaliD

Founded: 2016
Funding: €5.25M
Specialization: Digital ID wallet that consolidates various IDs for easy access and use

National Cybersecurity Strategy: Cyber-Security Strategy adopted in 2016

National CERT: SI-CERT (ARNES)

Education: 4+ universities offering cybersecurity-related programs

BALKANS COUNTRIES

Kosovo, Albania, Montenegro, North Macedonia, BiH, Serbia

DEFENSE/DUAL-USE SECTOR	CYBERSECURITY SECTOR

STARTUPS

8	8

FOCUS AREAS

• AI & Machine Learning • Autonomous Systems & Robotics • Embedded Systems & Hardware Acceleration	• Vulnerability Management & Offensive Security • AI-Driven Physical Security & Surveillance • Zero Trust & Secure Access Management

TOTAL FUNDING

TOP 3 INVESTMENTS (APR 2022 - APR 2025)

01 Anari AI - €3.17M (2023)	**01** Secfix - €3.6M (2022)
02 N/A	**02** Trickest - €1.4M (2023)
03 N/A	**03** Skenify - €100K (2024)

MOST ACTIVE INVESTORS

No recurring investors	Innovation Fund Serbia

IMPORTANT PLAYERS

	Founded	Stage	Funding	Specialization
NOVELIC Acquired by Sona Comstar	2013	M&A	€461K	mmWave radar systems and perception solutions, specializing in embedded systems and semiconductors
SKAITECH	2020	N/A	N/D	Drone services and solutions, including manufacturing, customization, and training
Synapse Aviation	2016	Seed	€88K	Software solutions aimed at improving flight safety and efficiency in the aviation industry

TRICKEST (SERBIA)

Founded: 2020 **Stage:** Seed / Early-Growth

Specialization: All-in-one Offensive-Security Automation platform for attack-surface mapping, vulnerability scanning and custom red-team workflows

Team size (full time): 6 **Funding:** €2.9M

Investors: Credo Ventures, Earlybird Digital East Fund, plus angels Daniel Dines & Marius Tirca (UiPath)

Clients: Platform adopted by NVISO, Halborn and other MSSPs & enterprise red-teams

Startups to Watch: Machine Can See (Serbia), Skenify (Montenegro), Ylide (Serbia)

	KOSOVO	ALBANIA	MONTENEGRO	NORTH MACEDONIA	BiH	SERBIA
NATO	✗	✓	✓	✓	✗	✗
Defense Budget	€165.6M (1.48% GDP)	€500M (2.04% GDP)	€140M (2.02% GDP)	€327M (2.05% GDP)	€200M (0.9% GDP)	€2.15B (2.60% GDP)
National CERT	KOS-CERT	AL-CIRT (AKSK)	CIRT.ME	MKD-CIRT	No national CERT (only entity/sector)	SRB-CERT
Talent & Education	~3 universities & 1 military academy with cyber/tech curricula	~5 universities & 1 military academy with cyber/tech curricula	~1 university & 1 military academy with cyber/tech curricula	~5 universities & 1 military academy with cyber/tech curricula	~7 universities & 1 military academy with cyber/tech curricula	~9 universities & 1 military academy with cyber/tech curricula

SLOVAKIA

DEFENSE/DUAL-USE SECTOR	CYBERSECURITY SECTOR

STARTUPS

10	10

FOCUS AREAS

• Robotics & Automation • Advanced Sensors & Materials • Embedded Hardware & Wireless	• Identity and Access Management (IAM) • Blockchain and Post-Quantum Security • Threat Protection & Infrastructure Security

TOTAL FUNDING

TOP 3 INVESTMENTS (APR 2022 - APR 2025)

01 InoBat - €100M (2024) **02** Picogrid - €10.56M (2024) **03** CulturePulse - €1.5M (2025)	**01** elv.ai - €500K (2024) **02** N/A **03** N/A

MOST ACTIVE INVESTORS

IPM Group & Neulogy Ventures	Neulogy Ventures & CB Investment Management

IMPORTANT PLAYERS

	Founded	Stage	Funding	Specialization
InoBat	2019	Series-C	€137.34M	Specializes in R&D and manufacture of custom-designed electric batteries for automotive, commercial vehicle, motorsport, and aerospace sectors
Picogrid	2020	Seed	€11.53M	Develops a unified platform for unmanned systems.
SEC Technologies	2014	Series-A	€3.21M	Produces advanced stand-off detection technologies with a focus on prevention, safety, and internal control

2024 Defense Budget: ~ €2.63 billion (2.00% of GDP)

Key international ties/partnerships:
EU CSDP, PESCO, Visegrád Group, Bilateral cooperation with Czechia and the U.S.

Education: 1 national military academy with tech/cyber curricula

ESET

Founded: 1992 **Stage:** Private, profitable

Specialization: Endpoint protection, threat intelligence, antivirus, and enterprise cybersecurity solutions

Team size (full time): 2000+ **Funding:** Bootstrapped (privately held, no external VC)

Clients: Over 110 million users in more than 200 countries and territories

Startups to Watch: elv.ai, 3IPK, Crayonic

National Cybersecurity Strategy: National Cyber-Security Strategy 2021-2025

National CERT: SK-CERT

Education: 2 universities offering cybersecurity-related programs

CZECH REPUBLIC

DEFENSE/DUAL-USE SECTOR	CYBERSECURITY SECTOR

STARTUPS

7	26

FOCUS AREAS

- Immersive Simulation & Training
- Space Analytics & Connectivity
- Advanced Air Mobility & UAS Management

- Identity & Access Management (IAM)
- AI-Driven Threat Detection & Behavior Analytics
- Vulnerability & Infrastructure Security

TOTAL FUNDING

TOP 3 INVESTMENTS (APR 2022 - APR 2025)

01 Vrgineers - €5.28M (2023)
02 ZAITRA - €1.7M (2024)
03 STRATOSYST - €761K (2024)

01 IP Fabric - €23.1M (2023)
02 Threat Mark - €20.24M (2025)
03 Whalebone - €13.35M (2025)

MOST ACTIVE INVESTORS

ESA BIC Czech Republic & CzechInvest	Credo Ventures & Fazole Ventures

IMPORTANT PLAYERS

	Founded	Stage	Funding	Specialization
ZAITRA	2020	Pre-Seed	€1.66M	Utilizes artificial intelligence for enhanced data processing in space
Vrgineers	2017	Series A	€11.21M	Develops and manufactures advanced virtual and mixed reality headsets and simulators tailored for professional pilot and defense training
Dronetag	2018	Seed	€651K	Offers an all-in-one solution for safe drone flights, enabling compliance with European and US regulations

IP FABRIC

Founded: 2015 **Stage:** Series B

Specialization: Automated network discovery, assurance, intent verification, compliance, and drift detection through Network Digital Twin (NDT) technology

Team size (full time): 100+ **Funding:** €27.07M

Investors: One Peak Partners, Senovo, Presto Ventures, Credo Ventures

Clients: 100+ global enterprises (Airbus, Red Hat, Major League Baseball, MLB)

Startups to Watch: Whalebone, Resistant AI, Ellio

2024 Defense Budget: ~ €6.38 billion (2.10% of GDP)

Key international ties/partnerships:
EU CSDP, PESCO, Visegrád Group, Bilateral cooperation with Germany and the U.S.

Education: 1 national military university (University of Defence in Brno) with cyber/tech curricula

National Cybersecurity Strategy: Cyber-Security Strategy 2023-2028 + action plan 2021-25

National CERT: GovCERT.CZ (NUKIB)

Education: 20+ universities offering cybersecurity-related programs

ESTONIA

DEFENSE/DUAL-USE SECTOR	CYBERSECURITY SECTOR

STARTUPS

13	44

FOCUS AREAS

- Autonomous Aerial & Surveillance Systems
- Situational Awareness & Command Platforms
- Secure Communications & Mission Control

- Identity & Access Management (IAM)
- Cybersecurity Education & Workforce Development
- Threat Detection, Intelligence & Automated Response

TOTAL FUNDING

TOP 3 INVESTMENTS (APR 2022 - APR 2025)

01 Frankenburg Technologies €4M (2025)
02 SensusQ - €3.8M (2024)
03 GScan - €3M (2025)

01 Blackwall - €45M (2025)
02 RangeForce - €17.60M (2023)
03 Binalyze - €16.72M (202

MOST ACTIVE INVESTORS

ESA BIC Estonia	Startup Wise Guys & Passion Capital

IMPORTANT PLAYERS

	Founded	Stage	Funding	Specialization
Milrem Robotics	2013	M&A	N/A	Autonomous unmanned ground vehicles (UGVs) for defense and civilian applications
Wayren	2020	Series A	€7.88M	Communication platform for uninterrupted connectivity in challenging environments
Frankenburg Technologies	2024	Seed	€3.83M	Advanced missile systems that are more affordable and faster to produce, utilizing an AI-powered situational awareness platform

2024 Defense Budget: ~ €1.33 billion (3.43% of GDP)
Key international ties/partnerships:
EU CSDP, PESCO, Nordic-Baltic Cooperation (NB8), Bilateral cooperation with Finland, Sweden, and the U.S., Cyber Defense cooperation via CCDCOE
Education: 1 national military academy (Estonian National Defence College) with cyber/tech curricula

VERIFF

Founded: 2015 **Stage:** Growth (Series C)

Specialization: AI-powered identity verification and fraud prevention for KYC, onboarding, and compliance.

Team size (full time): 450+ **Funding:** €170M

Investors: NordicNinja VC, Ace Ventures, Tiger Global Management, Accel, Index Ventures, Y Combinator, Superangel, Mosaic Ventures, Change Ventures, SV Angel, Alkeon Capital, IVP

Clients: 1,000+ globally across fintech, crypto, mobility, gaming, and e-commerce sectors (e.g., Bolt, Starship, Deel, Uphold)

Startups to Watch: Salv, Patchstack, Glassity

National Cybersecurity Strategy: Cyber-Security Strategy 2023-2027
National CERT: CERT-EE (RIA)
Education: 4 universities offering cybersecurity-related programs (as of 2025)

LITHUANIA

DEFENSE/DUAL-USE SECTOR	CYBERSECURITY SECTOR

STARTUPS

8	17

FOCUS AREAS

- Unmanned Systems & Drones
- Photonics & Laser Technologies
- AI & Autonomy

- Identity Verification, Digital Trust & Compliance
- Consumer & Personal Cybersecurity Tools
- Threat Detection, Risk & Infrastructure Security

TOTAL FUNDING

TOP 3 INVESTMENTS (APR 2022 - APR 2025)

01 Aktyvus Photonics - €4.2M (2025)
02 Unmanned Defense Systems - €3.1M (2024)
03 Granta Autonomy - €1M (2024)

01 Nord Security - €88M (2023)
02 Ondato - €3.61M (2023)
03 CyberUpgrade - €2.5M (2024)

MOST ACTIVE INVESTORS

Coinvest Capital & ScaleWolf	Founderheads & FIRSTPICK

IMPORTANT PLAYERS

	Founded	Stage	Funding	Specialization
Unmanned Defense Systems	2022	Seed	€3.98M	Specializes in advanced loitering munitions, battlefield situational awareness, and swarm technology solutions, integrating AI-based UAV swarms with modern battle management systems
Brolis Semiconductors	2011	Growth	€10M	Develops and manufactures advanced semiconductor optoelectronic devices and electro-optical systems for defense and security applications
Rubedos	2009	Seed	€956K	Develops 3D visual perception and navigation technology for vision-guided robotics applications across various industries

NORD SECURITY

Founded: 2012 **Stage:** Late Stage VC

Specialization: Cybersecurity suite for consumers and businesses, including VPN, password management, cloud access security, and encrypted file storage

Team size (full time): 200+ **Funding:** €184M

Investors: General Catalyst, BaltCap, Warburg Pincus, Burda Principal Investments, Audrey Capital, Illusian, Tesonet, Novator

Clients: 15M+ users across 20+ countries, including enterprises, remote teams, and privacy-focused consumers

Startups to Watch: Ondato, CyberUpgrade, idBlender

2024 Defense Budget: ~ €2.4 billion (3.12% of GDP)

Key international ties/partnerships:
EU CSDP, PESCO, Visegrád Group, Bilateral cooperation with Germany and the U.S.

Education: 1 national military university with cyber/tech curricula

National Cybersecurity Strategy: Cyber-Security Strategy adopted in 2018

National CERT: CERT-LT / NCSC

Education: 8 universities offering cybersecurity-related programs

LATVIA

DEFENSE/DUAL-USE SECTOR	CYBERSECURITY SECTOR

STARTUPS

8	6

FOCUS AREAS

• AI-Guided Precision Munitions • Radar & Vision-Based Targeting • Rapid-Deploy Autonomous Weapons	• Identity Authentication • Secure Communication Platforms • Digital Document Security & Signing

TOTAL FUNDING

TOP 3 INVESTMENTS (APR 2022 - APR 2025)

01 Origin Robotics - €4M (2024) **02** Lightspace Labs - €750K (2022) **03** N/A	**01** Handwave - €566K (2024) **02** N/A **03** N/A

MOST ACTIVE INVESTORS

Latvian Ministry of Defence Grant Programme	No recurring investors

IMPORTANT PLAYERS

	Founded	Stage	Funding	Specialization
Origin Robotics	2022	Seed	€8.21M	Develops advanced UAV systems for defense
Lightspace Labs	2014	Seed	€11.01M	Develops advanced AR headsets that offer high-resolution 3D imaging
Atlas UAS	2015	Late Stage VC	€7.04M	Designs and manufactures autonomous UAV systems for defense, security, and industrial applications

2024 Defense Budget: ~ €1.35 billion (3.3% of GDP)

Key international ties/partnerships:
EU CSDP, PESCO, NB8, Bilateral cooperation with Nordic countries and the U.S., Baltic Defense Cooperation

Education: 1 national military academy with cyber/tech curricula

REGULA

Founded: 1992 **Stage:** Growth / Established Private

Specialization: Forensic devices and software for document authentication, biometric verification, and border security

Team size (full time): 300+ **Funding:** Bootstrapped

Investors: None (Privately owned)

Clients: 1,000+ clients in 150+ countries, including Interpol, Frontex, banks, airlines, and border control agencies

Startup to Watch: ALTER

Founded: 2023
Funding: €7.87M
Specialization: Cybersecurity solutions for AI applications and chatbots

National Cybersecurity Strategy: Cyber-Security Strategy 2023-2026

National CERT: CERT.LV

Education: 6 universities offering cybersecurity-related programs

Ukrainian Defense Tech in 2024: Battlefield-Proven and Maturing

Den Smyrnov
CEO, CPO & Co-Founder of The Defender Media

Roman Sudolsky
Founding Editor of The Defender Media

Over the past five years, the world has been living through a continuous stress test: war on Europe's borders, energy insecurity, a global pandemic, supply chain fragility, and rapid technological escalation. In times like these, innovation accelerates – not just for defense, but for resilience. From GPS to the internet, some of the most transformative technologies of the last century began as military tools. The same could be true today.

Presto Tech Horizons is betting on that future. Backed by venture firm Presto Ventures and industrial group Czechoslovak Group (CSG), the fund aims to invest €150 million in dual-use, defense, and security technologies from NATO countries and allies. Its thesis: investing in resilience is not just about protection – it's about enabling breakthroughs across logistics, manufacturing, energy, healthcare, and beyond.

Specifically, investments in defense technology reached €52 million last year, accounting for 13% of total investments in Ukraine's tech ecosystem. The actual figure may be even higher, as many deals in the sector remain undisclosed.

In 2025, investments in Ukrainian defense tech could surpass €88 million – almost doubling compared to 2024.

KEY FACTS AND FIGURES[1–4]

PRODUCTION CAPACITY

6x

times compared to 2023

Arms production volume

2022: €0.88B

2023: €2.63B

2024: €8.8B

FORECAST FOR 2025: €26.31B

+800

Enterprises involved

+300K

Defense specialists

New weapon models

+1K

with

Made in Ukraine

50%

Share of ukrainian-made arms in the armed forces

30%

The Ukrainian defense tech ecosystem grows around Brave1

Private investors became significantly more active in Ukrainian defense technology in 2024, but it's the governmental cluster Brave1 that remains responsible for the majority of defense technology investments in the field. Almost €35 million were spread from its grant fund in 2024. Overall, in the two years since its inception, Brave1 has already provided more than 500 grants to developers, totaling over €42 million.

Brave1 serves not only as a grant fund. It's also the largest incubator and accelerator for startups in the field, providing support with codification, legislation, networking, and securing military contracts. In just two years, an entire ecosystem of Ukrainian defense tech has emerged, uniting over 1,500 teams and more than 3,600 products. About 80% of technological products used by the Ukrainian military today were born 'within the walls' of Brave1, says Nataliya Kushnerska, CEO of Brave1.

Brave1 is responsible for creating entire verticals within the market, such as Ukrainian UGVs (Unmanned Ground Vehicles) and EW/ELINT (Electronic Warfare/ Electronic Intelligence). Two years ago, there was no codification process for private initiatives in these fields. Brave1 helped make this happen, and today, more than 50 electronic warfare products have been codified, including those from Kvertus, UNVAWE, Rebel Group, mudro.tech, and Abakus Tech. The same goes for UGVs. There were three manufacturers two years ago, and now there are almost 70 products.

“It’s amazing to see that concept come to life and make such a significant contribution. Thanks to Brave1, more teams have emerged, and they’re progressing toward building products faster – and it’s not just about the money. It’s also about access to military expertise and the community,” says ***Anton Verkhovodov,*** *partner at D3, one of the most active funds in Ukrainian defense tech.*

Private funds and accelerators

Defence Builder aims to connect Western investors and Ukrainian defense technology startups to jointly fund the future of defense innovations.

"Ukrainian innovations are changing the industry with advanced tech solutions, and many Western technologies are being enhanced based on battlefield requirements in Ukraine, setting a quality standard for militaries worldwide,"
*– **Daria Yaniieva,** Head of Defence at Sigma Software Group, which is one of Defence Builder's founders.*

In terms of private investments in Ukrainian defense tech, the most active funds include D3, MITS Capital, NEZLAMNI Fund, Green Flag Ventures, Angel One Fund, and Double Tap Investments.

Angel One Fund participated in 7 syndicate deals involving Ukrainian defense tech startups in 2024. Medium checks of the fund's investments in those deals ranged between € 50,000 and € 200,000. Till the end of the year, the fund plans to close five more deals. "We would especially like to highlight our two most recent investments: Frontline and Norda Dynamics – they are relatively young but growing very quickly," highlighted Ivan Petrenko, Managing Partner of Angel One Fund.

Recently, Frontline also received investment from Germany's Quantum Systems and entered into a strategic partnership with them."At the turn of 2024/25 and now, I see the irreversibility of international collaboration – not just in terms of entering new markets, but also technological integration and the use of global R&D capabilities," Ivan commented. Among the most mature projects, he highlights Swarmer, Skyeton, Airlogix, and Himera.

*"Our defense tech market has matured and now has a better understanding of what it needs," – **Ivan Petrenko**, Managing Partner of Angel One Fund.*

Deborah Fairlamb from Green Flag Ventures says the fund specifically looks for scalable product companies founded in Ukraine that offer innovations in dual-use military, cyber, and AI technology. "We focus on early-stage investments (pre-seed through Series A) with ticket sizes between €100K - €600K. We prioritize startups whose wartime experiences have given them strategic and tactical advantages that can be translated to broader international defense and commercial markets."

According to Fairlamb, investing in wartime innovations is important because the experience these companies have accumulated provides them with a unique competitive advantage in rapidly developing and battle-testing new technologies.

The real-world validation of their innovations positions these companies favorably for rapid adoption in adjacent markets, especially across NATO and Eastern European countries that face similar security threats.

What trends dominated Ukrainian defense technology in 2024? Ivan Petrenko, Managing Partner of Angel One Fund points out three key ones:

01 A second wave of young startups has emerged – they're developing their products quickly and without the mistakes made by earlier pioneers.

02 The technological level of teams has increased.

03 Many manufacturers have shifted their focus from building entire systems (such as an ATGM - Anti-Tank Guided Missile or a drone) to finding their niche and working on specific components, including communications and optics.

In 2024, European investors also became more active in the Ukrainian defense tech market. One example is Czech-based Presto Tech Horizons which backs companies that enhance not just state and institutional security, but also personal safety and data privacy. Their ticket sizes range from *€300,000 to €5 million*, with a sweet spot around €2 million.

Almost a year since its inception, the Presto Tech Horizons fund has already welcomed its first four portfolio companies, including two Ukrainian defense tech startups – Vidar Systems, known for its portable acoustic locators, and Bavovna.ai, a hybrid AI platform for autonomous drone navigation.

"If you're a Ukrainian founder in defense, your motivations are through the roof. You want to survive. You want to win the war. That's dedication on a whole different level. And it's crucial – because in the early stages, talent and motivation are everything. That's what really matters. So this is a huge plus when it comes to the attractiveness of Ukrainian companies,"
*– **Matej Luhovy**, an investor at Presto Ventures.*

He admits that Ukrainian hardware manufacturers still have a lot to learn to grow, though there are some top-level projects in the communication field and electronic warfare. *"The way Ukrainian drones communicate with ground stations, the mechanisms they use to avoid jamming, and the location systems that prevent*

drones from crashing when jammed – these are areas where Ukraine might be the number one manufacturer of such technologies in the world," Luhovy concludes.

Building the Drone Valley

Dozens of different defense tech sectors are developing in Ukraine, but UAV manufacturing makes up the lion's share of the market. Serial entrepreneur **Yaroslav Azhnyuk** believes Ukraine has a chance to become the world's "Drone Valley," much like Silicon Valley in California. Before the full-scale invasion, Azhnyuk was building a successful pet startup called Petcube, which raised €22 million in investments. Now, he runs two defense tech companies: the Odd Systems project produces thermal imaging cameras for drones, while Fourth Law develops software for UAVs – specifically, AI-based guidance systems.

In 2024, over 2 million UAVs were produced in Ukraine alone.

The scale of drone manufacturing in Ukraine is truly impressive. In 2024, over 2 million UAVs were produced in the country, according to **Oleksandr Kamyshyn**, the President's advisor on strategic industries, speaking in March. The Ukrainian government predicts this number will grow to 3.5 - 4.5 million in 2025. According to the Ukrainian Arms Dealers Association, over 96% of all drones used by Ukraine's Defense Forces are domestically produced.

Commander-in-Chief of the Armed Forces of Ukraine Oleksandr Syrskyi noted that the supply of drones to the Ukrainian Armed Forces increased 19 times in 2024, and the number of enemy targets hit and destroyed increased by 3.7 times.

According to Data Driven, top 8 UAV manufacturers in Ukraine reached almost €132 million in net profit in 2024.[5] Among the biggest are Ukrspecsystems (SHARK drones), DeViRo (Ciconia, Rallus), Skyeton (Raybird), Athlon-Avia (Furia), SPE Ukrjet (Airborne, Topaz), TAF Drones (Colibri), Airlogix (GOR), and Vyriy. All the top companies are also working on the localization of manufacturing. In March 2025, Vyriy released the first 1000 drones made entirely from Ukrainian components.

The challenges: Money and technology

Despite the rapid growth of investments in Ukrainian defense technology, the market still lacks sufficient funding. Yaroslav Azhnyuk reminds that his previous company, Petcube, which develops high-tech entertainment for pets, raised €23 million in investments. In comparison, he points out that it is approximately the same as the total volume of private funding Ukrainian defense tech raised in 2024 (excluding grants from Brave1).

"Components are costly, and the development team is very expensive because it comprises many high-quality senior engineers – you can't solve this problem with juniors. Therefore, capital will significantly aid the development of Ukrainian defense tech if directed in the right way," says ***Ivan Kaunov****, Co-founder of Buntar Aerospace. – "Defense tech is not cheap, so we are talking about hundreds of millions."*

Another challenge is technology. Being in the early stages of its development, Ukrainian defense tech could greatly benefit from partnerships with major players from abroad. *"Quite frankly, if we compare hardware companies – what's being built in the U.S. versus in Ukraine – it's still not at the top level,"* says Matej Luhovy from Presto Tech Horizon.

Combining technological expertise with Western partners would significantly help Ukrainian defense tech rise sharply. *"They have the technologies we need but don't always know how to use them in modern warfare. And we do,"* pointed Ivan Kaunov.

What to expect in 2025?

According to forecasts, in 2025, Ukrainian defense tech will focus on:

- strengthening missile and unmanned aerial vehicle programs;
- innovative technologies and strategic partnerships with Western countries;
- further development of unmanned technologies, production of 30,000 long-range drones
- production of 3,000 cruise missiles and drone missiles

In 2025, investments in Ukrainian defense tech could surpass €100 million – almost doubling compared to 2024.

REFERENCES

1. Defence Tech Breakthrough of the Year – The Defender Media
   https://thedefender.media/en/insights/defence-tech-breakthrough-year/
2. Share of Ukrainian-Made Weapons Reaches 30% – Ukrinform
   https://www.ukrinform.net/rubric-defense/3970758-share-of-ukrainianmade-weapons-reaches-30.html
3. Report on the Results of the Defence Industry in 2024 – UCID (Ukrainian Center for Defense Innovations)
   https://ucdi.org.ua/en/news-en/report-on-the-results-of-the-defence-industry-in-2024/
4. Ukraine Accelerates Weapons Production: 'We Produce More Howitzers Than All of Europe Combined' – El País
   https://english.elpais.com/international/2025-04-08/ukraine-accelerates-weapons-production-we-produce-more-howitzers-than-all-of-europe-combined.html
5. The Top 8 Ukrainian UAV Manufacturers – LinkedIn (GroupDataDriven)
   https://www.linkedin.com/posts/groupdatadriven_the-top-8-ukrainian-uav-manufacturers-activity-7320773163817091072-OHY4/


WE NEED TECHNOLOGY,
NOT MEN ON THE
BATTLEFIELD

Tech, Not Men, on the Battlefield: A New Era of Asymmetrical Warfare

Author: Teodora Atanasova

In the war-torn fields of Ukraine, the reality of modern warfare is changing. Traditional military doctrines – built around mass mobilization and manpower – are being rewritten by engineers and coders. The frontline has become a testing ground for drone swarms, electronic warfare, battlefield AI, and autonomous systems. Ukraine's military, vastly outnumbered, is fighting a war it cannot win with manpower alone.

The new doctrine is stark and urgent: we need tech, not men, on the battlefield. ***We need tech to save the men.***

This shift is being shaped daily by soldiers and engineers. We spoke with three people at the heart of this transformation: a defense-tech founder building systems under fire, who wished to remain anonymous (we'll call them B.); Yurii, a frontline officer in Ukraine's 3rd Assault Brigade; and Andrii Buzarov, Ukrainian political analyst and legal advisor.

"You'll Never Match Russia's Manpower – So Don't Even Try"

"We'll never have enough people to match Russia's approach to warfare, especially large-scale, manned assaults," says B. "So we must focus on asymmetrical weapons to level the playing field."

Russian forces, B. notes, have enormous drone-manufacturing capacity and sophisticated electronic warfare systems. "They're not incompetent. They're adapting fast. We have to match their pace – and then exceed it."

> The problem, B. explains, is that most current innovations are linear: detect a drone's frequency, jam it, wait for them to change it, and start over. "It's a cat-and-mouse game. A reactive cycle. But real victory comes when you break that loop – when you build systems that adapt faster than the enemy can think," says B.

For them, the goal is to move from hacking one protocol to building tools that can hack any protocol, in real-time. "That's what I call an asymmetrical weapon. It's not about killing more – it's about making the enemy's tools irrelevant," also adds the tech founder.

And yet, much of today's defense innovation, B. warns, is dangerously disconnected from battlefield realities. "You can't build effective defense tech from outside Ukraine, or without military people on the team. You're just building something and hoping it works. That's not enough."

"You Don't Learn to Fight with Drones in School"

Yurii, a senior officer in the 3rd Assault Brigade, echoes this perspective from the front line. "Most of the people who join the military today are learning in the field. That's where the real, critical, hands-on knowledge comes from," he explains. "We're trying to train new people as fast as we can – but the battlefield moves faster."

> When asked what Ukraine needs the most right now, his answer is clear: "Autonomous systems. That's how we survive the asymmetry in manpower, equipment, and even strategy."

UAVs are one success story – most produced locally. By April 2025, Ukraine's Deputy Defense Minister Valerii Churkin stated that over 95 % of drones "currently used at the front line" were Ukrainian-made.[1] But even these take time to deploy. Despite talk of lightning-fast innovation cycles, Yurii is skeptical. "Two weeks? That would be a dream. We're working hard to shorten that loop – but real battlefield deployment takes time."

The biggest obstacle isn't technical – it's practical. "If you don't design tech with soldiers from the start, it won't work. It might be brilliant in theory but useless in practice. Developers need to see how we fight, how we charge devices, how terrain affects performance."

That's why his brigade works directly with startups and engineers – to test, break, and improve systems in combat. "The faster that loop from lab to trench, the more lives we save," explains Yurii.

"You Can't Regulate War After the Fact"

But as these technologies explode in scope and speed, ethical and legal questions follow closely behind. "Governments can't afford to be reactive anymore, they need to be proactive," says Andrii Buzarov.

> "The battlefield is already filled with experimental AI and drone systems. But laws haven't caught up."

He sees great potential in AI and autonomous tools for training, support, and even logistics – but warns against letting automation override human judgment." AI follows pre-programmed steps. It can't improvise. It can't be ethical and reason things. That's why I believe AI should support soldiers – but never fully replace them in critical decisions."

Most crucially, he says, autonomous weapons should be treated with the same caution as chemical or biological arms. “We need global legislative frameworks – fast. What’s being tested in Ukraine today could be in any conflict tomorrow.”

Redefining what it means to fight

The idea “tech, not men” isn’t about removing humanity from war. It’s about saving it. It’s about designing smarter ways to defend freedom, especially when facing an enemy that treats soldiers as expendable.

Ukraine doesn’t have the manpower to win a war of attrition. But it does have the ingenuity to fight smarter, faster, and more surgically. And that ingenuity – if supported with resources, regulation, and real-time battlefield collaboration – could shape a new model for 21st-century defense.

> “You win not by matching the enemy – but by making their strengths irrelevant,” says the founder.

In this new world, success won’t be measured by battalions deployed or tanks destroyed. It will be measured by how fast a drone was adapted, how accurately a signal was intercepted, and how intelligently a system responded before a human even had to act.

This is not science fiction. It’s the war unfolding now.

And in that war, the side that puts engineers' wits on the front line will win.

REFERENCES

1. “Ukraine Uses Over 95 % Domestically-Made Drones on Front Line, Deputy Defense Minister Says” – The Kyiv Independent https://kyivindependent.com/ukraine-uses-over-95-of-domestically-made-drones-at-front-line-defense-ministry-says/

Bronia.ai: Acoustic AI as the Next Line of Defense

TODOR TODOROV

CEO, Bronia AI

As drone threats grow in complexity, traditional radar, and camera-based detection systems are revealing critical blind spots – particularly in urban environments, low-altitude zones, and covert operations. Sofia-based Bronia.ai emerges as one of the most advanced CEE deep tech startups, addressing these gaps with a novel, acoustics-first approach to situational awareness. Bronia's Sonic.Guard platform introduces a new paradigm in counter-UAV and dual-use sensing by leveraging intelligent edge microphones and cloud-based AI.

Unlike active systems that emit signals and are prone to detection or interference, Sonic.Guard operates passively, identifying drones and other threats through acoustic signatures – even beyond line of sight. This positions Bronia's technology as a compelling solution for both defense and civil use cases, from border surveillance and artillery reconnaissance to smart city gunshot detection and environmental monitoring.

The system's modular architecture allows for fixed, mobile, or autonomous deployment, and its compact footprint (low SWaP - size, weight, and power) enables rapid deployment in under 10 minutes by a single operator. The detection range extends up to 250 meters for standard UAVs, with larger ranges for bigger threats. Once a sound of interest is captured, Bronia's AI platform executes a full "detect–triage–respond" cycle - localizing, classifying, and alerting relevant teams or systems via a cloud-native app ecosystem.

In addition to counter-drone capabilities, Bronia.ai's Sonic.Guard platform addresses the growing threat of gun violence with its new advanced acoustic gunshot detection system, designed for both military and civil scenarios – including school safety. Traditional systems relying on delayed 112/911 calls or misidentified sounds often fall short.

Bronia’s passive, AI-enhanced solution detects and classifies gunshots within seconds, identifies weapon type and direction, and localizes the shooter with up to 30-meter accuracy – even in complex urban soundscapes. For vulnerable sites like school campuses, Sonic.Guard can be deployed as a fixed or autonomous sensor mesh, enabling real-time alerts and tactical insights while remaining undetectable to attackers.

Built by a team of engineers and Ivy League-affiliated PhDs, Bronia combines model interpretability, ethical AI principles, and sensor fusion for secure and scalable deployment. As demand for dual-use technologies accelerates across NATO and EU-aligned markets, Bronia’s strategy to bridge civil and military applications could make it a key player in Europe’s defense AI stack.…

CYBER WARFARE:
THE NEW BATTLEFRONT

Cyber Warfare at the Threshold: Strategy and Alliances in Flux

Author: Ana Marija Kostanić

The shape of modern warfare is changing. Cyber operations are no longer support tools or low-level espionage – they are now central instruments of state power, integrated into military doctrine, political strategy, and economic disruption.

From battlefield coordination in Ukraine to persistent state-on-state digital pressure, the nature of cyber warfare is evolving fast. But understanding this evolution requires more than just a technical perspective. As Robin Dimyanoglu, cybersecurity expert and author of Geopolitical Cyber Threat Intelligence, puts it:

> *Cybersecurity is a socio-technical discipline. It sits at the intersection of technology, politics, and human behavior.*

So, let's examine the core dynamics: how the Ukraine war reset assumptions about cyber conflict, why digital operations now mirror Cold War rivalries, how international coordination is evolving, and what emerging technologies are doing to tilt the balance.

Ukraine and Russia: A case study in cyber

The Russia–Ukraine war has been the most visible example of cyber warfare used in direct coordination with military force. What's unique is not just the number of cyberattacks – it's how they were timed and layered with kinetic strikes. This coordination marked a shift: cyber was no longer just about espionage or nuisance disruptions; it became a battlefield enabler.

In February 2022, hours before Russian troops crossed the border, Russian actors launched a cyberattack on Viasat KA-SAT terminals.[1] This was a military-grade operation: it disrupted satellite communications for both the Ukrainian military and civilian users across Europe. At the same time, Russian groups carried out denial-of-service (DDoS) and wiper malware attacks on Ukraine's government and financial institutions. The aim was simple: confuse, isolate, and disable the Ukrainian state just as the invasion began.

Yet, the results were mixed. Ukraine, backed by its cyber teams and a coordinated defense effort by U.S. and European allies, adapted quickly.[2] Tech companies like Microsoft and Cloudflare provided cloud migration, threat intelligence, and DDoS mitigation almost in real-time.[3] Ukraine's CERT responded to more than 4,000 cyber incidents in 2023 alone, many linked to Russian intelligence units like Sandworm and Fancy Bear.[4]

The Ukraine conflict underscored that cyber operations are not isolated disruptions but tools for shaping operational tempo. With a solid foundation of intelligence and scenario planning, cyber becomes more than a reaction – it becomes a proactive and integrated strategic instrument.

Navigating Cold War in the cyber domain

Unlike conventional war, cyber conflict rarely reaches a dramatic flashpoint. Instead, it is characterized by continuous low-level engagement—probing, disrupting, stealing, and surveilling. In this way, it mirrors the strategic logic of the Cold War: constant pressure below the threshold of open war. Chinese actors like Volt Typhoon increasingly target U.S. critical infrastructure, mapping vulnerabilities in power grids and ports.[5] Russian groups pursue hybrid operations blending malware with influence campaigns.[6]

U.S. Cyber Command's "defend forward" posture – actively operating in foreign networks to detect and disrupt threats before they reach U.S. infrastructure – signals a strategic pivot in cyber deterrence. Rather than relying solely on the promise of retaliation, this approach aims to impose friction on adversaries by continuously engaging them in contested digital terrain.[7] While "defend forward" is a technical maneuver, it is also a geopolitical statement: it asserts presence, builds pressure, and narrows the adversary's options by anticipating intent, not just reacting to action. The logic behind this shift aligns with Dimyanoglu's observation that cyber threats cannot be fully understood without accounting for their broader strategic context.

Europe, while generally more regulatory and resilience-focused in its approach, can draw valuable lessons from the U.S. model of persistent engagement. U.S. Cyber Command's assertive posture has shown how early disruption and proactive defense can limit an adversary's freedom to maneuver. While Europe may be slower to adopt offensive cyber operations due to legal and political constraints, initiatives such as the EU Cyber Rapid Response Teams[8] and exercises under the PESCO framework[9] suggest that there is momentum building.

Dimyanoglu supports that simulations and wargaming exercises are crucial as they prepare participants for unexpected situations like breakdowns in communication, trust, and tool interoperability.

"I think the most effective training modules are the ones that simulate end-to-end incident response in a way that reflects real world complexity. Drills that go beyond isolated technical scenarios and instead stress test full incident response procedures are key. These help SOC teams get used to operating in environments where decisions need to be made quickly, even when the picture is still incomplete."

The increasing integration between national and sectoral CSIRTs, alongside coordinated drills and information-sharing platforms, shows that Europe is already evolving toward a more dynamic cyber posture – though its operational doctrines are still maturing in contrast to the more operationalized U.S. stance.

International threats require international cooperation

However, no single nation can defend against cyber threats alone. Infrastructure is global, attackers are transnational, and attribution is complex.

"Another area we need to train more deliberately is pivoting from indicators to broader campaign patterns. SOC analysts should be comfortable asking: Is this a standalone incident, or part of a wider operation? That shift in thinking is what helps teams recognize when something local might actually require a coordinated, EU-level response," emphasizes Robin Dimyanoglu.

Over the years, and especially in the recent ones, multilateral defense has grown more operational:

01 NATO's Tallinn-based Cooperative Cyber Defence Centre of Excellence (CCDCOE) coordinates the annual Locked Shields cyber defense exercise, simulating real-time attacks on national infrastructure with participation from over 30 countries.[10]

02 EU Cyber Rapid Response Teams launched under PESCO are deployable across EU member states during crises to support national CERTs in real-time. Practical response mechanisms are outlined in the EU Cyber Solidarity Act.

03 The U.S. Joint Cyber Defense Collaborative (JCDC) integrates private companies (like Microsoft, CrowdStrike, and Google) with federal agencies to provide real-time threat intelligence and defense.[11]

Dr. Vilius Benetis, Director of Lithuanian NRD Cyber Security and active ecosystem builder and researcher explains that trust-driven relationships remain at the core of collective resilience:

"Following social and professional trust – coming from diverse partnerships, and facilitating business relationships – those are the best foundations to build and experiment with new capabilities, collective resilience, incident response and information sharing."

Across Central and Eastern Europe (CEE), national Critical Information Infrastructure (CII) sensor deployments highlight another layer of cooperation and challenge. Benetis explains: *"CII sensors are deployed in the region in each North European country, sometimes even across several sensor networks. One is managed by the national cybersecurity center, another by a sectorial monitoring and incident response team, and the other is operated by commercial SOC partners. The discipline of network sensors has been practiced for many years already in the region, and they are a crucial part of both monitoring and incident response processes."*

He notes that while regulatory frameworks facilitate formal cooperation, much of the real readiness stems from cross-sector exercises and grassroots communities. Afterall, rapid pivoting from local incidents to EU-level alerts requires both technical acumen and contextual awareness. To top it off, Dimyanoglu emphasizes the need to train SOC analysts to think strategically:

> *"Sometimes the timing, the target, or the TTPs (Tactics, Techniques, and Procedures) make more sense when viewed through a geopolitical lens."*

Beyond the technical lens

Most cyber professionals come from technical backgrounds. Dimyanoglu points out that this can be a blind spot: *"When we approach this domain purely through a technical lens, we miss a significant part of the picture."*

Integrating Signals Intelligence (SIGINT), Human Intelligence (HUMINT), and Open Source Intelligence (OSINT) requires more than collecting data; it requires making sense of it in strategic terms. Dimyanoglu advocates for cross-disciplinary collaboration: *"A cyber threat intelligence team might benefit greatly from understanding how a military analyst interprets escalation dynamics."*

This shift isn't about converting engineers into political analysts, but about fostering shared frameworks for interpretation. Dimyanoglu references PMESII/ASCOPE[12] and DIMEFIL[13] as useful tools to connect geopolitical variables to attack scenarios. "*They all essentially aim to map out the same thing: the broader operational environment (political, military, economic, social, informational, infrastructure) and how shifts in any of those layers might trigger a certain course of action*," he adds.

Beyond these, a number of advanced cyber threat intelligence models are increasingly blending operational analysis with geopolitical foresight. For instance, the MITRE ATT&CK framework[14], while traditionally technical, is being adapted in some circles to map not only techniques but also align them with nation-state motivations and timing related to political events.

"What I find most useful is when you combine this structured environmental analysis with pattern-based observations from historical data. In the case of something like the Russia-Ukraine conflict, cyber activities are fairly well documented. Once you start clustering those events by attack types, targeted sectors, or regional focus, and then overlay them onto a framework like PMESII, you start to see clearer lines between geopolitical objectives and how cyber operations might have been used to support them," explains Robin Dimyanoglu.

In parallel, industry leaders and academic researchers are experimenting with hybrid methodologies that integrate threat modeling with open-source geopolitical trend analysis to predict timing, target selection, and escalation thresholds. These combined approaches reflect a growing recognition: without structured frameworks that encompass both the technical and geopolitical layers, cyber intelligence risks becoming siloed, reactive, and incomplete.

Caution, though: not all threats come from nation-states. Criminal syndicates and hacktivists often exploit geopolitical flashpoints without formal state backing. Distinguishing between opportunism and state intent is a core analytical challenge.

Cyber warfare today is *not* a standalone discipline

It is deeply embedded in the logic of modern conflict. As Dimyanoglu puts it: "*At the end of the day, it's about building the muscle memory to go from local action to joint response without losing speed.*" This requires more than technology. It requires a mindset shift: seeing cyber not just as a technical space, but as a geopolitical toolset. Organizations must layer their defenses with insight – not just logs and alerts, but narratives, patterns, and intent. Benetis underscores as well, the strength of cyber defense doesn't just come from tools and sensors, but from trust, community, and sustained engagement: "*It relies on how strong the local and regional cybersecurity ecosystem is.*"

REFERENCES

1. "Cyberattack on Viasat" – CyberPeace Institute
   https://cyberconflicts.cyberpeaceinstitute.org/law-and-policy/cases/viasat
2. "The Threat of Russian Cyberattacks Looms Large" – The New Yorker
   https://www.newyorker.com/news/daily-comment/the-threat-of-russian-cyberattacks-looms-large
3. "Defending Ukraine: Early Lessons from the Cyber War" – Microsoft
   https://cdn-dynmedia-1.microsoft.com/is/content/microsoftcorp/microsoft/msc/documents/presentations/CSR/Defending-Ukraine-Early-Lessons-from-Cyber-War.pdf
4. "A Russian Cyberattack Knocked Out Kyivstar. Its Effects Are Still Rippling Through Ukraine" – WIRED
   https://www.wired.com/story/ukraine-kyivstar-solntsepek-sandworm-gru
5. "Volt Typhoon: Nation-State Threat Targeting Critical Infrastructure" – CybelAngel
   https://cybelangel.com/volt-typhoon/
6. "People's Republic of China State-Sponsored Cyber Actor Living off the Land to Evade Detection" – CISA
   https://www.cisa.gov/news-events/cybersecurity-advisories/aa24-249a
7. "Cyber 101: Defend Forward and Persistent Engagement" – U.S. Cyber Command
   https://www.cybercom.mil/Media/News/Article/3198878/cyber-101-defend-forward-and-persistent-engagement/
8. "Cybersecurity: EU Strengthens Cyber Defence Capabilities and Cooperation" – European External Action Service (EEAS)
   https://www.eeas.europa.eu/node/47525_en
9. "Cyber Rapid Response Teams and Mutual Assistance in Cyber Security" – PESCO (Permanent Structured Cooperation)
   https://www.pesco.europa.eu/project/cyber-rapid-response-teams-and-mutual-assistance-in-cyber-security/
10. "Locked Shields" – NATO Cooperative Cyber Defence Centre of Excellence (CCDCOE)
    https://ccdcoe.org/locked-shields/
11. "CISA Launches New Joint Cyber Defense Collaborative" – CISA
    https://www.cisa.gov/news-events/news/cisa-launches-new-joint-cyber-defense-collaborative
12. "Planning Templates" – U.S. Marine Corps Training Command (MCCMOS)
    https://www.trngcmd.marines.mil/Portals/207/Docs/wtbn/MCCMOS/Planning%20Templates%20Oct%202017.pdf?ver=2017-10-19-131249-187
13. "Utilization of the DIMEFIL Framework: A Case Study Analysis of Security Cooperation Success" – Small Wars Journal
    https://smallwarsjournal.com/2020/11/08/utilization-dimefil-framework-case-study-analysis-security-cooperation-success/
14. "MITRE ATT&CK: Applying the Framework" – IBM
    https://www.ibm.com/think/topics/mitre-attack

Making Attackers Try Harder: How Pentest-Tools.com Brings Offensive Tactics to the Right Side of the Fight

Cyberattacks across Europe are becoming faster, stealthier, and more frequent. From healthcare and transport to finance and public services, state-backed actors and ransomware groups increasingly target the essential infrastructure that keeps societies running. In this evolving threat landscape, defenders must act before attackers do.

Pentest-Tools.com, a cybersecurity company founded in Romania, is helping security teams do just that. It enables organizations to pinpoint and validate vulnerabilities across their most exposed assets - websites, APIs, networks, and cloud environments - before those weaknesses are exploited. The core mission is clear: equip defenders to find and fix the problems that matter most, before attackers get in.

Built by reverse-engineering the attacker mindset

What differentiates Pentest-Tools.com is **how deeply** it draws from the offensive playbook. Rather than simply reacting to known risks, the product builds on reverse-engineering how attackers think. Every capability - authenticated scanning, asset discovery, custom exploit validation - is modeled on real-world intrusion tactics.

This approach gives defenders an edge. By replicating the logic and behavior of adversaries, Pentest-Tools helps security teams close critical gaps earlier, validate high-risk exposures, and focus remediation efforts where they'll make the biggest difference. It's an attempt to flip the traditional dynamic - making attackers work harder, and defenders smarter.

"Our goal is to build tools that reflect how real attackers examine their targets - because that's how security teams make decisions that matter. What secures Europe's future - and everyone else's - isn't just more automation. It's experienced people using the right tools to understand risk and act with precision."

ADRIAN FURTUNA

Founder & CEO,
Pentest-Tools.com

More than 2,000 security teams across 119 countries have adopted the company's tools. These users range from individual consultants and internal security teams to managed service providers. In 2024 alone, customers ran over 6.3 million scans and automated more than 611,000 penetration testing sequences using the pentest robots.

What draws such a wide user base is not just the breadth of scanning capabilities, but the ability to reduce noise. The product delivers pre-validated findings with proof-based reporting, helping teams avoid time-consuming false positives and focus on what's actionable. For many customers, it's a way to scale efforts without compromising on speed or clarity.

Trusted by 2,000+ security teams in 119 countries

2000

Security teams using the product across 119 countries

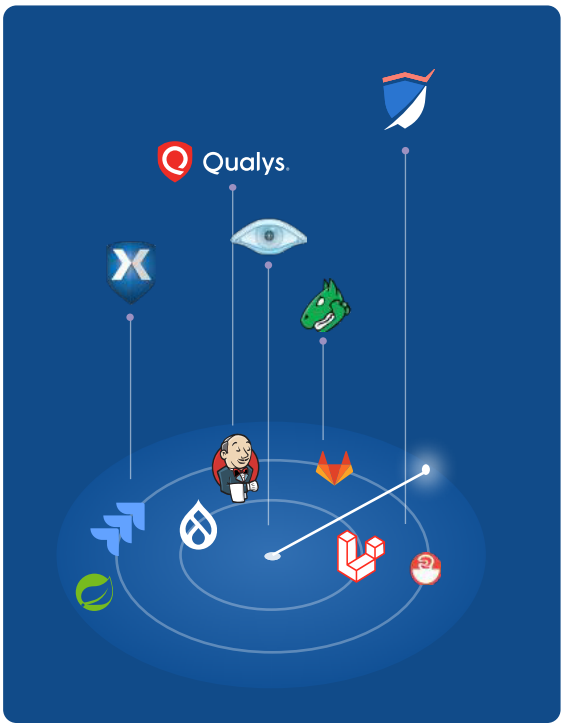
6.3M

Scans performed by customers in 2024

611.000

Penetration testing sequences automated

The company's performance is not based on promises alone. In recent independent benchmarks, Pentest-Tools.com ranked first in detection accuracy across 167 test environments in the network vulnerability scanners benchmark. It also outperformed legacy tools in identifying verified flaws in the web application vulnerability scanners benchmark.



One standout example is its Password Auditor, which succeeded in identifying weak credentials in 84% of test cases - compared to just 15% for a leading open-source alternative. These results reflect a consistent engineering focus on precision, speed, and attacker-level insight - outcomes rooted in deep offensive security expertise and ongoing product development.

Built in Europe. Ready for what's next.

While the company's reach is global, its foundations are European. As more governments and enterprises look to reduce their dependency on foreign cybersecurity providers, companies like Pentest-Tools.com are demonstrating that competitive, high-performance tools can be built and scaled from within the region.

The team's long-term vision is to help build a digital environment where defenders stay ahead, not behind. That means making the cost of compromise higher for attackers - and building a more resilient, better-protected Europe in the process.

Top-ranked Accuracy

RANKED

#1

167 test environments (network scanner benchmark)

84%

Weak credentials detected (Pentest-Tools Password Auditor)

50%

Reduction in false positives (web app testing) with ML

NAVIGATING TECHNOLOGIES IN CYBERSEC

Technologies in CyberSec: Bringing Opportunities – And Risk

Author: Ana Marija Kostanić

Cybersecurity in 2025 is at a pivotal juncture, shaped by the rapid evolution of artificial intelligence (AI), quantum computing, and cloud technologies. These advancements offer transformative opportunities for enhancing security but also introduce complex risks that organizations must navigate. We delve into the current landscape, highlighting key developments and providing strategic insights for preparation.

First things first, do you trust your supply-chain?

Cyberattacks through the software supply chain are growing faster than any other threat – and most companies are still unprepared. A 2024 report by ReversingLabs found a 1,300% increase in malicious packages on public code repositories since 2020, with many targeting AI and cryptocurrency projects.[1]

One reason the numbers continue to climb is that attackers are playing a long game. The XZ Utils backdoor (CVE-2024-3094) lay dormant in a Linux compression library for two years while its maintainer quietly climbed the trust ladder.[2] When activated, it could have allowed full control over many Linux systems if it hadn't been caught just in time. These "slow burn" threats exploit hidden risks – like overworked volunteers maintaining critical software, unknown dependencies buried deep in code, or build processes that trust upstream code without verifying it.

Effective third-party cyber risk management relies on robust reporting and visibility, yet most firms still "watch the river with binoculars". According to the BlueVoyant 2024 report, there has been a notable 25 % decrease (from 44% in 2023 to 19% in 2024) in regular monthly-or-better reporting, indicating a critical gap that needs addressing.[3] Traditional questionnaires or annual audits can't keep up with modern software development, where thousands of packages may be added to public repositories every day.

At the same time, artificial intelligence is reshaping how supply-chain threats work – on both sides. Attackers now use AI to create fake or misleading packages that appear safe, targeting high-interest keywords like "LLM" or "crypto." But defenders are also getting smarter. As Igor Lasić, SVP of Technology at Croatia's black unicorn ReversingLabs, explains, their platform, Spectra Assure, uses machine learning to scan software binaries (even without source code) and detect malware before release.

Other companies are building similar “early warning” systems to detect suspicious behavior among suppliers, and governments are also taking action now.[4] The European Cyber Resilience Act, which took effect in late 2024, will require all companies selling digital products in the EU to provide software bills of materials (SBOMs), report vulnerabilities within 24 hours, and prove their software is “secure by design” – or face penalties starting in 2027.[5] But even these steps aren’t perfect – researchers have shown that some SBOM tools can be tricked, giving organisations a false sense of security if verification isn’t built in.[6]

Trust in your supply chain isn’t about checking a box – it’s about ongoing oversight and shared responsibility. Companies that invest now in smarter monitoring, stronger partnerships, and clearer standards will not only reduce their own risk but also gain an advantage as regulators and customers demand greater transparency and security by default.

AI’s double life in cybersecurity

As mentioned, AI has significantly reshaped cybersecurity dynamics. In 2025, the impact of AI is evident in both the rapid evolution of threats and the swift responses of organizations.

On the offensive side, large language models (LLMs) and generative AI are lowering the skill barrier for cybercriminals. Attackers now automate the creation of tailored phishing emails, deepfakes, and polymorphic malware that adapts to avoid detection. And these AI-driven attacks are no longer fringe experiments. Between 2023 and 2025, phishing success rates improved by 55% when powered by generative AI.[7] Emerging models like Google’s Veo-3 can even generate highly realistic deepfakes, further complicating incident response and enabling more effective disinformation or impersonation during crises.[8]

A less visible but growing issue is the security of the AI tools themselves. Axios reports that the average enterprise now uses 66 generative AI tools, many of which are introduced without formal review or security assessment.[9] These tools often process sensitive data, connect to cloud infrastructure, or integrate into development pipelines. Without governance, they can expose organizations to data leakage, model poisoning, or backdoors.

At the same time, AI is delivering decent advances in defense. Platforms like ReversingLabs use machine learning to protect AI itself. Igor Lasić describes how the company scans serialized machine learning models (e.g., Python Pickle files) for embedded malicious code – a tactic seen in recent threats like the “nullifAI” malware uploaded to Hugging Face.[10] Their system flags unsafe behaviors such as remote command execution or unauthorized network calls during model deserialization – an overlooked risk as enterprises scale AI use without securing the models themselves.

AI also helps analysts by summarizing large volumes of telemetry, attributing threats from minimal data, and creating targeted protections. However, these benefits come with limitations. Even well-trained models rarely exceed 90% reliability in real-world conditions, and must be continuously tested and retrained to remain effective.[11]

This challenge becomes critical when AI is used for automated response. If a system acts on flawed insights – escalating rather than containing an incident – the consequences can be severe. That's why many teams still rely on human analysts to verify AI-driven alerts, particularly in high-risk environments.

> *"We have an abundance of data, but what we found challenging is accuracy. Even with using the appropriate prompting, it is necessary to have additional AI agents test the accuracy of the produced answers,"* says Igor Lasić, Reversing Labs

Another concern is alert overload; without careful tuning, even the best AI models can overwhelm analysts or mask real threats behind noise. Despite these risks, AI remains essential. A 2025 Darktrace survey found that 95% of cybersecurity professionals believe AI has significantly improved threat detection, incident response, and overall resilience.[12] Self-healing endpoints, AI-assisted SOC triage, and real-time threat correlation are increasingly common in mature security programs.

The key is to use AI as an amplifier – not a replacement – for human judgment. Organizations must implement clear governance for AI models, monitor model drift and accuracy, and maintain human oversight for critical decisions. Periodic testing, lineage tracking, and red-teaming of AI tools should become standard practice – especially as attackers also begin targeting AI systems themselves.

The encryption expiry date

Quantum computing is no longer a far-off scientific concept – it's a near-term issue with real implications for cybersecurity. While general-purpose, fault-tolerant quantum computers capable of breaking current encryption standards have not yet been built, progress is consistent, visible, and well-funded. As Anastazija Pažin, cybersecurity consultant and PhD researcher in post-quantum cryptography (PQC), says, the threat is not science fiction anymore – it is real, and it is strategic.

> *"While large-scale quantum computers capable of breaking RSA and ECC are not available yet, we are witnessing consistent progress from both public and private sector actors. The risk does not lie in the exact moment of quantum supremacy but in the fact that critical data, encrypted today, can already be intercepted and stored for future decryption. The urgency comes not from what quantum computers can do today but from what we are not doing to prepare for their tomorrow,"* warns Anastazija Pažin.

"European organizations should begin by identifying which of their assets are "quantum-vulnerable" and adopt crypto-agile strategies. This means upgrading systems to handle new algorithms, conducting cryptographic inventories, and piloting PQC in non-production environments. EU bodies such as ENISA, ANSSI, and BSI are already encouraging these steps – it is time others follow." – Anastazija Pažin

This is the core of the "harvest now, decrypt later" (HNDL) threat. Adversaries – particularly nation-states – are intercepting and storing encrypted traffic today to decrypt it when quantum capabilities mature. This places any long-term sensitive data – such as diplomatic communications, health records, financial transactions, and intellectual property – at risk of exposure in the coming decade. The cryptographic algorithms most at risk are RSA, ECC, and DSA.

These systems underpin most secure communications today, from HTTPS and VPNs to authentication and digital signatures. Once large enough quantum computers are built, these algorithms can be broken, which solves integer factorization and discrete logarithm problems exponentially faster than any classical method.[13] That makes current cryptography obsolete for long-term security use – even if it remains unbroken today.

While the arrival timeline of quantum machines capable of breaking public-key cryptography is still debated, most estimates fall between 5 and 15 years, points Pažin. "That said, crypto migration is not plug-and-play. It takes years to redesign, test, and deploy quantum-safe architectures across complex systems – especially in regulated industries." The migration effort itself can take just as long; therefore, it is even more critical for organizations to begin now.

Unfortunately, preparation remains low. A 2025 ISACA survey found that 67% of European IT professionals believe quantum computing will change cybersecurity risk in the next ten years. Still, only 4% of organizations have a formal strategy in place.[14]

"Preparedness varies significantly. Some defense and national security organizations are proactively investing in quantum-resistant architectures and policies. The financial sector, due to regulatory pressure, is beginning to move – slowly but surely. The challenge is not awareness – it is execution. What is needed is an alignment of funding, mandates, and practical tooling. The EU has strong frameworks, but they must be enforced at scale." – Anastazija Pažin

Several nations are moving ahead with offensive and defensive quantum strategies. In the U.S., NIST finalized the first set of Post-Quantum Cryptography (PQC) standards in 2024, for broad deployment in government and industry systems.[15] China, for example, has deployed a 4,600 km quantum communication network, including space-based QKD links.[16] Meanwhile, in Europe, The European Quantum Communication Infrastructure (EuroQCI) is underway, aiming to build a secure quantum network across all 27 EU countries—including space-based QKD via ESA and terrestrial fiber segments.[17]

These provide a sound foundation for transition, but few players in the private sector are currently "crypto-agile" – capable of updating cryptographic algorithms without major architectural redesign. This is where emerging players may help fill the gap. Pažin is optimistic about the role of European innovation:

> *"Startups in Europe – and especially in the CEE region – are agile, innovative, and often closer to the problem than larger vendors. We are seeing exciting developments in key management, quantum entropy generation, lightweight cryptography, and post-quantum VPNs. However, scalability and funding remain concerns. That said, I am optimistic. If these startups are supported with the right ecosystem – pilot opportunities, public-private partnerships, inclusion in EU research programmes – they will not only be ready, but could lead Europe's strategic autonomy in PQC."*

No trust in a multi-cloud world

Today, in 2025, nearly every industry depends on cloud infrastructure for scalability, agility, and real-time data access. But as organizations continue to shift critical workloads into public, hybrid, and multi-cloud environments, the risks associated with cloud security are evolving in depth and complexity. These challenges are amplified by rapid change, decentralized control, and an expanding attack surface that includes everything from misconfigured APIs to AI model exposures.

Cloud environments offer unique advantages – particularly around infrastructure visibility and centralized control. Cybersecurity researcher and author Robin Dimyanoglu notes that cloud-native environments integrate identity, network, endpoints, and applications, allowing security teams to enforce unified policies more effectively than in fragmented, on-premises systems. However, this tight integration can also create a single point of failure:

> *"The cloud effectively integrates all aspects of an IT environment… This means that if one component is compromised, the attacker can potentially move laterally across the entire system with much greater ease, especially if permissions and access controls aren't robustly managed."* – Robin Dimyanoglu

Gartner estimates that by the end of 2025, **99%** of cloud security failures will result from customer misconfigurations, not provider faults.[18]

IBM reports that **15%** of all breaches stem from cloud configuration errors.[19]

Wiz Research shows **31%** of active cloud deployments contain serious security flaws such as open storage buckets, exposed admin interfaces, and over-permissive roles.[20]

One of cloud's greatest strengths – agility – is also one of its greatest liabilities. Continuous deployment pipelines and auto-scaling infrastructure mean systems change faster than security teams can review them. As Dimyanoglu puts it:

> *"Cloud technologies enable rapid deployment and innovation, which is a significant advantage for organizations in fast-moving markets. But this agility comes with a trade-off: more frequent changes often introduce more vulnerabilities."*

This rapid pace of change is reflected in the high volume of security events reported. According to Snyk's State of Cloud Security Report, nearly 80% of organizations experienced at least one cloud security breach, and 27% reported public cloud incidents in just the past year.[21] IBM pegs the cost of a typical misconfiguration or credential-based breach between €3.8 million and €4.3 million – a figure that has steadily risen year over year.[22]

Nowhere is the shift in cloud security more evident than in identity and access management (IAM). As applications and infrastructure become API-driven and increasingly automated, identity-based controls are the primary gatekeepers. Yet enforcement remains inconsistent. Simultaneously, the integration of AI into cloud platforms has introduced entirely new layers of risks like insecure APIs, unmonitored models, and shadow AI.[23]

Another systemic challenge is the shared responsibility model. Cloud providers secure the underlying infrastructure, but customers are responsible for their data, configuration, and access controls. This boundary often leads to dangerous misunderstandings or gaps in coverage. Dimyanoglu warns:

> *"By relying on cloud providers, organizations offload some security responsibilities. But they also expose themselves to new risks, including supply chain attacks… [which] introduce dependency on external entities whose security practices are not always transparent or under your control."*

Lastly, the trend toward multi-cloud adds a layer of operational fragmentation. 79% of enterprises now operate across more than one cloud provider, increasing the risk of configuration drift, inconsistent policy enforcement, and gaps in telemetry. Tools that work on one platform may not function effectively across others, especially when orchestrated by siloed teams.

Dimyanoglu concludes that cloud security must move away from traditional layered defense models and toward a holistic, integrated architecture. Zero-trust principles – continuous verification, least-privilege access, and segmentation – are essential to contain lateral movement in cloud-native environments.

REFERENCES

1. "Software Supply Chain Security Report 2024" – ReversingLabs; https://www.reversinglabs.com/sscs-report-2024
2. "Reported Supply Chain Compromise Affecting XZ Utils Data Compression Library (CVE-2024-3094)" – CISA; https://www.cisa.gov/news-events/alerts/2024/03/29/reported-supply-chain-compromise-affecting-xz-utils-data-compression-library-cve-2024-3094
3. "The State of Supply Chain Defense 2024" – BlueVoyant; https://www2.bluevoyant.com/StateofSupplyChainDefense2024
4. "How LLMs Are Shaping Cybersecurity" – Financial Times; https://www.ft.com/content/1d07a823-43da-4c1b-84d3-7e453ebb1b16
5. Cyber Resilience Act – European Commission; https://digital-strategy.ec.europa.eu/en/policies/cyber-resilience-act
6. "Large-Scale Adversarial Testing of LLMs" – arXiv; https://arxiv.org/html/2412.05138v1
7. "AI-Powered Phishing vs. Humans" – Hoxhunt; https://hoxhunt.com/blog/ai-powered-phishing-vs-humans
8. "Google's New Veo-3 AI Can Generate Deepfakes—and Misinformation" – TIME; https://time.com/7290050/veo-3-google-misinformation-deepfake/
9. "AI Security Playbooks Must Catch Up" – Axios; https://www.axios.com/2025/06/06/ai-security-playbook-change-speed
10. "ReversingLabs Identifies Malware in Machine Learning Model Hosted on Hugging Face" – https://www.reversinglabs.com/blog/rl-identifies-malware-ml-model-hosted-on-hugging-face
11. See 4.
12. "The State of AI in Cybersecurity 2025" – Darktrace; https://www.darktrace.com/the-state-of-ai-cybersecurity-2025
13. "Thirty Years Later, a Speed Boost for Quantum Factoring" – Quanta Magazine; https://www.quantamagazine.org/thirty-years-later-a-speed-boost-for-quantum-factoring-20231017/
14. "Quantum Computing's Rapid Rise Is a Risk to Cybersecurity and Business Stability" – ISACA; https://www.isaca.org/about-us/newsroom/press-releases/2025/quantum-computings-rapid-rise-is-a-risk-to-cybersecurity-and-business-stability
15. "NIST Releases First 3 Finalized Post-Quantum Encryption Standards" – NIST; https://www.nist.gov/news-events/news/2024/08/nist-releases-first-3-finalized-post-quantum-encryption-standards
16. "Experimental Satellite Quantum Key Distribution" – Nature; https://www.nature.com/articles/s41586-020-03093-8
17. "European Quantum Communication Infrastructure (EuroQCI)" – European Commission; https://digital-strategy.ec.europa.eu/en/policies/european-quantum-communication-infrastructure-euroqci
18. "Is the Cloud Secure?" – Gartner; https://www.gartner.com/smarterwithgartner/is-the-cloud-secure
19. "Cost of a Data Breach Report" – IBM; https://www.ibm.com/reports/data-breach
20. "Cloud Data Security Report Snapshot" – Wiz; https://www.wiz.io/blog/cloud-data-security-report-snapshot
21. "Snyk's State of Cloud Security Report Reveals Organizations Have Experienced Severe Cloud Security Incidents" – Snyk; https://snyk.io/news/snyks-state-of-cloud-security-report-reveals-organizations-have-experienced-severe-cloud-security-incidents/
22. See 19.
23. "2024 State of Multicloud Security Risk Report" – Microsoft; https://cdn-dynmedia-1.microsoft.com/is/content/microsoftcorp/microsoft/final/en-us/microsoft-brand/documents/2024-State-of-Multicloud-Security-Risk-Report.pdf

Why Pen Testing Can't Be a Checkbox Anymore: Plainsea's Marko Simeonov on Building Continuous Security from the Inside Out

MARKO SIMEONOV
CEO of Plainsea

Penetration testing is still being treated by many organizations as a once-a-year compliance exercise – a box to tick rather than a meaningful security practice. But with cyber threats evolving daily and regulatory pressure mounting across Central and Eastern Europe (CEE), that mindset is becoming a dangerous liability for both governments and organizations.

In this interview, Marko Simeonov, CEO of Plainsea, explains why the traditional pen testing model is no longer fit for purpose and how his team is redefining it as a continuous, human-in-the-loop process. Simeonov also reflects on the cybersecurity challenges and opportunities in the CEE region and why building local resilience begins with empowering local talent and modernizing the tools they use.

What are the main limitations of traditional penetration testing models that Plainsea set out to overcome – and why do these limitations persist in so many organizations today? What mistakes do you usually observe?

The most common mistake is assuming penetration testing is simply a one-off project that functions as a compliance checkbox. This approach is fundamentally flawed because it fails to account for the dynamic nature of modern IT environments. Vulnerabilities can emerge daily, so treating pen testing as an annual or quarterly exercise rather than a continuous process is what keeps organizations always one step behind the adversary.

This is why, at Plainsea, we set out to challenge this model by enabling continuous penetration testing. Not just automating a few mundane tasks like other solutions do, but giving human testers the ability to stay embedded within the organization's testing lifecycle, adapt to infrastructure changes, and surface findings dynamically.

How does Plainsea's model of continuous penetration testing work in practice - and what does it change for both internal security teams and external testing providers?

Continuous pen testing means rethinking not just the testing cadence but the way the entire process is orchestrated, as I mentioned earlier. At Plainsea, we've built a platform that enables internal security teams and external testers to operate within a shared, unified system – where new assets, findings, risks, and priorities can be tracked in near real time.

For internal pen testing teams, this means far better control and visibility. They can triage, assign, and resolve issues as they appear and have everything in one place.

For service providers, it's an opportunity to offer new value – transforming a once-linear engagement into an ongoing partnership. And for both sides, it's a move toward real operational resilience.

Many cybersecurity platforms lean heavily into automation. How does Plainsea strike a balance between smart automation and the human expertise that's still critical in pen testing?

Automation should never be about eliminating the human from the equation - it's about reducing noise and optimizing manual work so the human can focus on the complex problems. For example, automating CVE enrichment or report generation can save hours of work. But identifying real-world risk? Contextualizing a business impact? That still requires human judgment to be interpreted.

With that idea in mind, at Plainsea, we've automated the parts that testers and clients alike find tedious: scoping, documentation, vulnerability information enrichment, CVE mapping, formatting, and reporting. That frees up ethical hackers to do what they do best - think creatively and critically.

How does Plainsea help security leaders move from reactive, ad-hoc security postures to a more proactive and measurable approach to risk reduction?

Proactivity in cybersecurity isn't just about finding vulnerabilities faster — it's about closing the loop. That means asking: are we reducing risk? Are we getting better over time? And can we prove it?

Plainsea helps leaders answer those questions with confidence. Our platform tracks trends across projects, business units, and even external providers. It brings consistency to reporting, structure to remediation, and accountability to the process.

When security becomes measurable, it becomes manageable. That's the shift - from reactive firefighting to strategic, continuous improvement.

What unique cybersecurity challenges or opportunities do you see emerging from the CEE region – and how is Plainsea positioning itself in this context?

Central and Eastern Europe (CEE) sits at a pivotal intersection of digital ambition and cybersecurity urgency. The region has become one of Europe's biggest investors in cybersecurity and defense technologies - and it's doing so in a context shaped by proximity to geopolitical tensions, growing regulatory pressure, and an increasingly sophisticated threat landscape. The result is a complex, fast-moving cybersecurity landscape - full of potential but also growing pains.

For all its momentum, the region still faces a serious disconnect between strong, yet limited technical talent and the operational maturity required to translate that talent into sustained resilience.

You'll find exceptional security engineers in places like Romania, Bulgaria, and Poland – professionals who could easily stand shoulder-to-shoulder with their colleagues worldwide. Yet, many operate within organizations where penetration tests are still commissioned only after an audit finding or a breach. Incident response plans often exist more on paper than in practice. Risk ownership is dispersed, and remediation workflows are rarely embedded into broader security strategies.

The result is that, on one hand, many organizations remain in a reactive posture, despite having the raw capability to do more. On the other – it creates a brain drain of CEE's cybersecurity workforce.

Lithuania, for example, continues to report major difficulties in hiring experienced cybersecurity professionals, with some positions remaining vacant for months despite competitive salaries. Similar shortages are being felt in Hungary, the Czech Republic, and across the region – especially as the NIS2 Directive and other EU-wide frameworks begin to raise the bar on accountability, reporting, and cyber readiness.

And yet – this isn't just a challenge – it's an opportunity. Countries like Estonia have demonstrated what's possible with integrated public-private cybersecurity ecosystems. Poland's MSSP sector is rapidly evolving, with more providers moving toward continuous testing and offensive security-as-a-service. Indigenous security companies like ESET and Safetech Innovations are proving that global-grade cybersecurity doesn't have to be imported – it can be grown right here.

All of this is proof CEE doesn't need to replicate the slower-moving enterprise security models of Western Europe. It has the chance to build leaner, smarter, and more agile service delivery models – if the tools and infrastructure allow it.

That's exactly where our platform is focused: giving service providers and security teams the operational backbone to offer scalable, continuous testing – without overwhelming resources or burning out existing talent.

We're not trying to "export Silicon Valley." We're building something grounded in the needs, speed, and strengths of the region.

Looking ahead, what's your vision for the future of penetration testing – especially as AI capabilities grow and compliance expectations evolve?

AI will help us scale – no question. It will generate payloads, simulate lateral movement, and even flag anomalous behavior that a human might overlook. But AI won't tell you WHY something matters in your specific context - that still requires a human analyst who understands business risk, not just system behavior.

What we're moving toward is a world where pen testing is no longer a periodic audit but a continuous and integral part of the security lifecycle. Compliance regimes like NIS2 and DORA are already nudging organizations in that direction - not just asking if a test was done, but how frequently, how effectively, and how findings translate into remediation and resilience.

I believe the next five years will be about transforming penetration testing into a strategic layer in enterprise risk management – integrated with CI/CD, aligned with risk governance, and enriched by AI in a way that elevates, rather than replaces, human expertise. That's how we'll keep up with adversaries who are already moving at machine speed – while still defending with human insight.

Kikimora: Making Professional Cybersecurity Accessible with AI Agents

Sofia-based cybersecurity company Kikimora is preparing to launch a next-generation software platform that leverages AI agents to streamline vulnerability management and compliance processes for companies across the CEE region. Set to debut in stages between mid-June and July 2025, the solution targets mid-sized enterprises (SMEs) that lack the resources to hire high-end cybersecurity specialists but face increasing regulatory and operational pressures.

At the heart of Kikimora's innovation is an MCP-based AI agent (Model Context Protocol), which allows organizations to locally deploy and manage AI models trained on public APIs like OpenAI while keeping sensitive data fully private. This setup is designed to meet the rising need for secure, private AI workflows in the face of evolving European cybersecurity regulations, including NIS2.

The AI agent simplifies one of cybersecurity's most complex challenges: prioritizing and acting on thousands of potential system vulnerabilities. Through a conversational interface, users can assign tasks, generate Jira tickets, and track remediation workflows with natural language prompts. Executives and non-technical users can also generate real-time compliance reports and manage documentation relevant to their industry or national regulations, streamlining oversight and governance.

According to IBM's 2024 AI report, organizations that utilize AI agents in cybersecurity can reduce breach-related costs by an average of €2 million and contain incidents nearly 100 days faster, particularly in larger enterprises. Internal experience and industry reports cited by Kikimora also show that context-aware AI can cut false positives by up to 90%, improving efficiency by reducing irrelevant alerts and freeing up teams to focus on higher-value tasks.

This product shift marks a strategic evolution of Kikimora's services model. The new value proposition reflects a broader trend in global cybersecurity: reducing operational complexity through automation and making advanced tools usable by non-specialists.

With a focus on privacy, automation, and accessibility, the solution reflects the growing demand across CEE for scalable cybersecurity tools that meet evolving regulatory and operational challenges.

Sign up for early access to Kikimora agents

How Warsaw Equity Group Is Fueling the Next Wave of Cybersecurity Scaleups in CEE

In an era of escalating digital threats and mounting geopolitical uncertainty, cybersecurity is no longer a vertical – it's a cross-cutting imperative. For Warsaw Equity Group (WEG), this shift marks a significant inflection point for the cybersecurity landscape in Central and Eastern Europe. The investment firm is placing its bets on scaleups that are not only technically sound but ready to move from local relevance to global resilience.

Scaling on Solid Ground

WEG's investment strategy is sharply defined. The firm backs B2B businesses with €2M+ in revenue, growing at a minimum rate of 20% annually, and is prepared to inject between €4M and €15M per deal, including both primary and secondary capital - usually as a minority stakeholder. But capital is only part of the equation. As Jan Nalbert, Investment Director at WEG, puts it

"We partner with companies entering a critical growth phase – those with the foundations in place, now looking to scale."

JAN NALBERT
Investment Director at WEG

To support this transition, WEG offers more than funding – when needed. A dedicated human capital lead works directly with portfolio companies to align their organizational design with growth goals, while WEG's team helps ensure that company vision and strategy translate into executable plans. This combination of flexible financing and hands-on organizational and strategic support is designed to help cybersecurity startups bridge the often-perilous gap between early traction and sustainable scale.

Why CEE? Why Now?

While U.S. firms still dominate the global cybersecurity landscape, CEE is gaining ground. **“Scaleups in the region are increasingly competitive,”** Nalbert notes, pointing to a deep pool of technical talent and growing specialization in underserved niches. **“CEE firms are no longer defined by low-cost engineering; today, they compete on the quality of their capabilities...”** This talent advantage, coupled with rising demand for digital sovereignty, especially among European enterprises and governments, plays to the region’s strengths.

Still, challenges persist. Late-stage capital remains scarce, regulatory environments vary significantly across countries, and establishing brand visibility on a global scale from CEE is more challenging. Talent retention is another structural barrier: even the most promising companies must compete with Big Tech for top-tier engineers.

A Playbook for Strategic Niches

Rather than attempt to dethrone the incumbents head-on, WEG sees opportunity in emerging sub-sectors and threat vectors that require a more agile, forward-looking approach to shape the market – domains where smaller, adaptable teams can move faster than enterprise giants.

A case in point is WEG’s recent investment in Xopero, a Polish company that began as a provider of backup software and has evolved into a leader in DevOps data protection with its GitProtect brand. What sets GitProtect apart is its specific focus on safeguarding developer platforms like GitHub, Jira, and Azure DevOps – critical, yet often overlooked, links in the cybersecurity chain. As regulatory demands increase and enterprises become more aware of the risks in relying solely on cloud providers, Xopero’s market is expanding. According to Nalbert, the company is gaining traction in both the U.S. and EU markets and could emerge as a category leader.

Looking Ahead: Consolidation and Cross-Border Expansion

WEG sees the next three to five years as a period during which early-stage ventures in CEE mature – some evolving into globally competitive players and strong contenders to their Western counterparts or even emerging as category leaders. Others may become attractive targets for cross-border M&A or strategic alliances. Western European and North American firms are expected to increasingly engage with CEE players to tap into their innovation, IP, and regional reach.

Moreover, the institutional ecosystem around cybersecurity in CEE is maturing. A growing number of local funds are now specializing in cyber and defense tech, and experienced founders – often repeat entrepreneurs - are building more ambitious companies from day one.

In a global environment where threats are escalating, and infrastructure is increasingly digital, the stakes for cybersecurity have never been higher. For Warsaw Equity Group, CEE's cybersecurity startups are not just underdogs – they're emerging contenders. Armed with deep technical expertise, niche focus, and the right kind of capital and support, these companies can build not only secure solutions – but secure futures.

Towards a More Cyber-Secure Europe: Preparing for the CRA

DIANA NITESCU
Founder OctogonHUB & Cybersecurity Consultant

The digital economy has already entered the era of emerging technologies. This shift raises the stakes for governance and risk management across all organizations.

Digital trust is the new capital. It's no longer enough to write smart code or build an innovative product. The real differentiator is: How "secure-by-design" is your digital environment? The Cyber Resilience Act, through a European cybersecurity certificate and label, raises the bar for every product, process, and team – from development and testing to delivery and post-market support.[1]

Who will benefit, and who will bear the cost of this cybersecurity reconfiguration into an integrated product and business architecture? With the CRA setting the highest cybersecurity standards globally, we explore how EU institutions, companies, and ecosystems are responding.

According to the OECD's Digital Economy Outlook 2024 – in terms of future digital strategies of its 38 member states – cybersecurity of digital devices, products, and services are set as one of the 5 key priorities.[2]

Among these, managed service providers (MSPs) have emerged as critical links – and targets, within the supply chain. As a result, states are focusing on two major response strategies:

Regulatory foundations.
Establishing institutional frameworks, cybersecurity policies, national incident response capacities, and safeguards for critical sectors (finance, energy, health, transport).

Technical and operational measures.
Implementing certification and labeling for digital products, reinforcing the supply chain, deploying Zero Trust models, and advancing cryptographic technologies such as homomorphic encryption and quantum systems.

Is the EU the most regulated cyber market?

Cybersecurity regulation in global markets began as early as 2002 with the introduction of the first ISO standards (ISO/IEC 62443), which have since evolved into a comprehensive framework of six cybersecurity standards covering a wide range of products, transportation, and customs control systems (ISO 27001, ISO/IEC 27002, ISO 28000, ISO/IEC 27036, ISO/IEC 20243, ISO/IEC 27019).

Over the years, regulations have become increasingly stringent, bolstered since 2015 by the adoption of region-specific frameworks: in the United States (CISA, NIST, Security America's Supply Chains), the United Kingdom (Product Security and Telecommunications Infrastructure Act), China (Cybersecurity Law, Data Security Law) and Singapore (Cybersecurity Act).[3–8]

The European Union stands out from other markets by establishing a cohesive and interconnected package of six mandatory cybersecurity regulations applicable to targeted companies across member states. The EU regulatory framework aims to build a European cybersecurity shield through the collective effort of its 27 member states, covering:

- Data protection (GDPR)
- Critical infrastructure (NIS Directive)
- Financial and banking sector resilience (DORA)
- Cybersecurity of digital products (Cyber Resilience Act - CRA)
- Governance of artificial intelligence in operations and products (AI Act)

The EU's approach to ensuring a robust cybersecurity shield is outlined in the Cyber Solidarity Act (CSA) and implemented through the European Cybersecurity Competence Centre (ECCC), headquartered in Romania.[9] The ECCC coordinates three Cross-border Security Operations Centres (SOCs), including the ENSOC Consortium (Spain, Italy, Luxembourg, Austria, Portugal, Romania, Netherlands) and the ATHENA Consortium (Bulgaria, Greece, Malta).

Understanding the trade-offs: Short-term strain, long-term strength

The CRA introduces significant changes that will initially strain EU economies and businesses:

- High technical compliance thresholds;
- Increased documentation and reporting;
- Higher operational costs;
- Legal liability assumptions;
- 24-hour incident reporting obligations;
- Complexity in adapting legacy and open-source products.[10]

Yet, these challenges are expected to yield meaningful medium- and long-term benefits:

- 30–50% increase in cybersecurity by 2029;
- 90% of EU products more cyber-resilient:
- Stronger market trust and user protection (B2B, B2G, B2C);
- Greater board confidence in digital investments;
- A safer, unified EU digital market.[11–12]

So, are EU countries ready for full CRA implementation by 2027? As of now, no. But the next 18 months are critical.

How are EU countries preparing for the CRA implementation?

EU member states have one and a half years until the full implementation of CRA standards. During this time, public-private partnerships are being established to reduce short-term impacts and maximize the opportunities brought by the CRA.

One of the outstanding initiatives is OSCRAT[13], an EU-funded project under the Digital Europe Programme, designed to provide SMEs with a free, open-source toolkit to facilitate compliance with the CRA. SECURE[14] is another EU-funded initiative aimed at enhancing the cyber resilience of SMEs. Coordinated by Italy's National Cybersecurity Agency (ACN), the project aims to provide financial support and resources to SMEs, helping them comply with the CRA.

Romania is also building two CRA platforms for SMEs: the CRACY platform[15], a partnership between Belgium, Romania, Greece, and Estonia, coordinated by the Romanian Authority for Digitalization and the CYBERFORT platform[16], a Romania–Cyprus partnership, developed under the coordination of the National Cyber Security Directorate of Romania. These platforms aim to enhance the cybersecurity and compliance readiness of European SMEs with the CRA by providing advanced technological solutions, compliance tools, and tailored training programs. Through a collaborative approach, both platforms will support SMEs in strengthening their cyber resilience and aligning with CRA requirements as well as other relevant standards such as ISO 27001, PCI DSS, and NIS2.

Many CEE countries are setting up training modules and guides for the implementation, keeping an open-line with the private sector for the feedback. For example, in the Czech Republic, NÚKIB (the Czech national CERT) began formal consultations with hardware/software vendors already in June 2024.[17] In the meantime, Czech suppliers are providing feedback on the draft list of “important” vs “critical” products so they know early whether third-party certification will apply. In March 2025, Croatia released the "CRA Guidelines for SMEs": a 35-page guide with fill-in templates for vulnerability policies and CE technical files.[18]

We anticipate that public-private efforts will accelerate across all EU Member States in order to meet the two key deadlines: 2026 (implementation and launch of vulnerability reporting for connected digital products) and 2027 (full implementation CRA) provisions in all companies that manufacture, import, distribute, or purchase hardware and software within the EU single market.

For a successful start, the Cyber Resilience Act Expert Group (CRA Expert Group) is being set up.[19] The expert group will assist and advise the Commission on issues relevant to the implementation of the Cyber Resilience Act (CRA)

How should EU companies prepare?

CRA will affect various entities. Corporations, small and medium-sized enterprises, startups, non-governmental organizations, government entities… No matter which, those entities are either affected by the CRA because they are developing and providing the technology that falls under the CRA, or they are buying and using it.

Companies should be also aware that some products do not fall under the scope of the CRA, as they are regulated by other cybersecurity laws or ISO standards: vehicles, aviation systems, medical devices, SaaS products, MVP/test-phase products, open-source software, military/defense systems, and applications developed for internal use.

In the next page you can see a full run-down of necessary steps companies – under CRA but also the end-user companies – should do and pay attention to.

Companies under CRA	End-user companies
Evaluate whether the product falls under the standards of the CRA	Need to inform themselves about: 1) CRA implementation status; 2) supplier evaluation and selection criteria
Determine if the product is *Critical/Normal* according to CRA standards	Introduce CRA obligations in supplier contracts
Implement the "Secure by design" model Starting from the Proof of Concept (PoC) stage. Policies, procedures, and actions are applied to strengthen the product's cybersecurity at every phase: design, development, testing, deployment, operation, updates & upgrades, uninstallation, incident reporting, etc.	**Only buy products that have:** • the EU cybersecurity label • an EU Declaration of Conformity • a Technical File including cybersecurity aspects • a defined security support/ update period • a security audit (internal, PenTest, ISO, etc.) • an incident reporting policy
Monitor, evaluate, and test the implementation of the "Secure by Design" model applied to the product under development (internal and external audits, penetration testing, etc.)	Assess security risks throughout their supply chain
Document each stage to demonstrate compliance with the Secure by Design approach and create a Technical File for each product	Request audits / Security Reports for critical products, those with AI and those purchased before the implementation of CRA
Submit the product's cyber file to obtain the EU Cybersecurity Certification and label	Monitor and respect update/ upgrade deadlines for purchased products
Monitor and perform periodic maintenance of product security	Organize training for staff (IT, procurement, legal) on the new CRA regulations
Notify customers of possible identified cyber vulnerabilities	Collaborate with the national cybersecurity authority
Notify cyber incidents to ENISA	

Opportunity for the startup ecosystem?

Even though the CRA puts unusual pressure on startups, they are still at an advantage compared to SMEs or well-established corporations in the ICT manufacturing, import, and distribution industry.

Imagine a startup in the early stages of product development – it can gain a competitive edge by adopting the "Secure by Design" model faster and more effectively.

Additionally, the startup business ecosystem is expected to develop fast-track solutions such as:

- **CRA Compliance as a Service**
  An integrated platform offering: security audits, automated documentation generation, attack simulations, testing and validation of CRA requirements.
- **CRA-ready marketplaces**
  App Stores / IoT Markets where users can search for CRA-certified products.
- **Automated system for cross-border conformity recognition**
  Recognition of CRA certifications by other jurisdictions (e.g., USA, UK, Canada).
- **CRA sandbox for innovators**
  Controlled environments where startups can test new products without CRA restrictions.
- **CRA Bug Bounty (crowdsourced security testing)**
  Programs supported by governments / the EU through which ethical hackers help identify vulnerabilities in digital products subject to the CRA.
- **Reuse of NIS2 and GDPR infrastructure**
  Many companies already have procedures and compliance teams in place for GDPR and NIS2. CRA requirements can be integrated into these existing workflows.
- **CRA Verified (digital labeling system)**
  Companies that adopt CRA early could gain benefits such as: priority access to public tenders, bonus points in innovation scoring / EU funding, etc.
- **Other innovations we have yet to imagine**

In 2025, cybersecurity will become the game-changer of digital transformation. Businesses no longer just sell products – they cultivate digital trust. Laws no longer constrain – they evolve into living architectures for emerging markets and dynamic governance. Be digital enough to unlock new connection points. Shape the future. Become a Cyber STAR. Jump and lead the shift.

REFERENCES

1. Cybersecurity Act – European Commission (Digital Strategy) https://digital-strategy.ec.europa.eu/en/policies/cybersecurity-act
2. OECD Digital Economy Outlook 2024, Volume 2 – OECD https://www.oecd.org/en/publications/2024/11/oecd-digital-economy-outlook-2024-volume-2_9b2801fc.html
3. Cybersecurity Information Sharing Act (CISA) – U.S. Congress https://en.wikipedia.org/wiki/Cybersecurity_Information_Sharing_Act
4. NIST SP 800-161: Supply Chain Risk Management Practices (2015) – National Institute of Standards and Technology; https://csrc.nist.gov/pubs/sp/800/161/r1/final
5. Product Security and Telecommunications Infrastructure (PSTI) Act 2022 – UK Government https://www.gov.uk/government/publications/the-uk-product-security-and-telecommunications-infrastructure-product-security-regime
6. Telecommunications (Security) Act 2021 – Parliament of the United Kingdom
7. Cybersecurity Law – Standing Committee of the National People's Congress https://en.wikipedia.org/wiki/Cybersecurity_Law_of_the_People%27s_Republic_of_China
8. Cybersecurity Act 2018 (amended by 2024 Bill) – Cyber Security Agency of Singapore & Parliament https://www.csa.gov.sg/legislation/cybersecurity-act
9. The European Cybersecurity Competence Centre https://cybersecurity-centre.europa.eu/index_en
10. European Cyber Security Organisation (ECSO). Streamlining Regulatory Obligations: CRA and Related EU Cybersecurity Regulations. December 2024. https://ecs-org.eu/ecso-uploads/2024/12/Streamlining-Regulatory-Obligations_10-Dec-2024_v2.pdf
11. ENISA. Cyber Resilience Act – Implementation of EUCC and its Applicable Technical Elements. https://certification.enisa.europa.eu/publications/cyber-resilience-act-implementation-eucc-and-its-applicable-technical-elements_en
12. GitProtect. Cyber Resilience Act: What Does It Mean for Your Digital Business? https://gitprotect.io/blog/cyber-resilience-act-what-does-it-mean-for-your-digital-business/
13. OSCRAT. Open Source Cyber Resilience Act Tooling Platform (OSCRAT); https://oscrat.eu/
14. Outsourcing Today. Cyber Resilience Act Could Trigger a New Regulatory Era for Software Companies in the EU; https://outsourcing-today.ro/?p=12432&
15. CRA-CY. Cyber Resilience Act – Cyprus Coordination Platform; https://cra-cy.eu/
16. CYBERFORT Project – National Directorate of Cyber Security (DNSC), Romania https://dnsc.ro/pagini/proiect-cyberfort
17. Czech National Cyber and Information Security Agency (NUKIB). https://portal.nukib.gov.cz/information-about-portal-nukib
18. OneTrust DataGuidance. Croatia: NCSC Publishes Guidelines on Cybersecurity and CRA Implications. https://www.dataguidance.com/news/croatia-ncsc-publishes-guidelines-cybersecurity
19. European Commission – Digital Strategy. Call for Applications: Cyber Resilience Act (CRA) Expert Group. https://digital-strategy.ec.europa.eu/en/news/call-applications-cyber-resilience-act-cra-expert-group

Nordic Recruitment & Consulting: Bridging Talent, Technology, and Security Across Europe

MIKKO SAARINEN
Founder and CEO

In the evolving landscape of cybersecurity, defense, and aerospace, Nordic Recruitment & Consulting is playing a key role in connecting talent, innovation, and strategic capabilities across Europe. Operating out of Bulgaria and Romania, the company delivers international recruitment and professional B2B staff leasing services with a core focus on IT, cybersecurity, and emerging defense technologies.

With a vetted network of over 37,000 IT professionals, Nordic Recruitment & Consulting supports both startups and established players in their growth, including firms working on cutting-edge cybersecurity and counter-drone solutions. The firm maintains active intelligence on sector trends, giving it a unique vantage point into how technologies like AI are reshaping the defense domain – particularly with the rise of autonomous drones and AI-enhanced weapon systems.

Among its high-profile partnerships is Gilat Satellite Networks, a global leader in satellite communications. Nordic serves as Gilat's official country partner in Bulgaria, recruiting for critical roles such as embedded systems developers and cybersecurity experts – including C-level positions.

Beyond talent services, the company offers custom end-to-end software development through a growing network of 34 specialized firms across Bulgaria, Romania, Ukraine, and North Macedonia. These partners encompass a diverse range of technical disciplines, including embedded development, telecom engineering, AI, computer vision, and drone systems.

Rounding out its offering, Nordic also provides cybersecurity testing services, including penetration testing, feature verification, and audit support – ensuring that clients not only build the right teams but also secure their infrastructure effectively.

By combining recruitment, custom software delivery, and security assurance, Nordic Recruitment & Consulting is helping CEE-based and international companies scale confidently into high-risk, high-tech sectors.

CONCLUSION:
FUTURE OUTLOOK

What Can Europe and the CEE Region Do Next?

As the geopolitical landscape hardens and the digital domain becomes increasingly contested, Europe faces a pivotal moment in shaping its cybersecurity and defense tech future. This moment is especially consequential for the Central and Eastern European (CEE) region, whose frontline position in current conflicts – geographic and digital alike – makes it both a vulnerability and a testbed for European resilience and innovation.

In cybersecurity, Europe represents one of the largest and most dynamic markets globally. Yet despite strong institutional support and rising awareness of cyber risk, the region's growth trails slightly behind global averages. The reasons are well-documented: high regulatory complexity, fragmented markets, and continued dependence on non-EU vendors.

These factors hit smaller players and CEE-based startups especially hard, preventing promising solutions from scaling and often forcing early-stage firms to seek acquisition or funding outside Europe. A more harmonized regulatory regime, aligned procurement standards, and a concerted effort to "buy European" would go a long way in mitigating these issues and leveraging the internal market's size globally.

In defense technology, the dynamic is inverted. Budgets are growing fast, especially in the Nordics and CEE, with many countries exceeding NATO's 2% of GDP spending targets. Public investment is surging – but private capital, particularly for later-stage ventures, remains scarce. Europe lags behind the U.S. and Asia in defense tech scaleups, partially due to conservative procurement systems and a historic aversion to dual-use commercialization.

Yet this is changing. Dual-use innovation – particularly in quantum, space, autonomous systems, and cybersecurity – is drawing increasing attention, and CEE states are emerging as significant players, with Ukraine's battlefield setting new standards for rapid, adaptive tech deployment.

Beyond these structural levers, Europe must build around its emerging advantages.

The regulatory instincts that once slowed growth – such as privacy protections, trust standards, and supply-chain scrutiny – are now becoming assets in a post-trust digital economy. Europe's ability to produce secure, interoperable, and regulation-friendly cyber and defense products is unmatched if paired with flexible implementation mechanisms.

Likewise, the hard-earned lessons from Ukraine provide a real-world testbed that no laboratory or sandbox can replicate. CEE's frontline innovations – drones, autonomous systems, battlefield communications – should be scaled continent-wide through EU-led consortia and standardized procurement channels.

Bridge the Procurement Gap

Governments across Europe, including in the CEE region, must move from passive equipment buyers to proactive ecosystem builders. That requires reforming procurement to favor agile, problem-first approaches that invite startups and SMEs into the fold. Creating faster pathways from pilot to purchase – mirroring US models like the Defense Innovation Unit – will be key. Defense ministries and EU institutions should coordinate to share risk in new tech deployments, especially in cross-border interoperability use cases.

Unlock Late-Stage Capital

While early-stage funding in European cybersecurity and defence tech is improving, late-stage financing remains a bottleneck. Europe can close this gap by activating its underused sovereign wealth, pension, and public investment funds. A dedicated EU cybersecurity and defence growth fund – backed by national and institutional investors – would reduce dependence on non-EU acquisitions and keep strategic technology within Europe's industrial base. This is particularly urgent for the CEE region, where a lack of local growth capital often pushes ventures abroad just as they reach global competitiveness.

Federate Operational Capabilities and Workforce Pipelines

The cyber talent gap is perhaps the most persistent threat to European resilience. Europe is structurally short on skilled cybersecurity labor, with a deficit of over 300,000 professionals. Instead of relying solely on long-term education reform, the EU and CEE countries must scale targeted reskilling programs and facilitate cross-border pooling of operational security resources. Federated Security Operations Centres (SOCs), supported by EU coordination, could offer shared capacity to public administrations and critical infrastructure providers, especially in smaller CEE states.

Beyond these structural levers, Europe must build around its emerging advantages.The regulatory instincts that once slowed growth – such as privacy protections, trust standards, and supply-chain scrutiny – are now becoming assets in a post-trust digital economy. Europe's ability to produce secure, interoperable, and regulation-friendly cyber and defense products is unmatched if paired with flexible implementation mechanisms.

Likewise, the hard-earned lessons from Ukraine provide a real-world testbed that no laboratory or sandbox can replicate. CEE's frontline innovations – drones, autonomous systems, battlefield communications – should be scaled continent-wide through EU-led consortia and standardized procurement channels.

Europe's strategic horizon is clear

Barring a dramatic easing in geopolitical tensions, both cybersecurity and defense tech will grow faster than global GDP through 2030. The question is whether Europe will remain a buyer of technology or become a co-leader in shaping it. If it can bridge the financing and procurement gaps, mobilize institutional capital, and integrate its fragmented efforts – especially across the CEE region – it can convert today's vulnerabilities into competitive strengths. The opportunity is not just to protect Europe but to build a sovereign, scalable, and exportable model of digital and strategic resilience for the democratic world.

Citation and Distribution Notice

When quoting or referencing information from the report "*Who is Protecting Europe's Future?*", please credit The Recursive as the source. Suggested citation format:

"*Who is Protecting Europe's Future?*, The Recursive, 2025.

Available at: https://therecursive.com"

We kindly request that you refrain from disseminating the report directly. Instead, please share the registration link to access the report.

While the report is free, sharing the link helps us understand and measure genuine interest in its content. For extended excerpts, permission must be obtained from The Recursive.

_____