



THE RESILIENCE CODE: From Vulnerability to Resilience – How Technology Can Promote Security and Defense in Europe

[The words of VDE CEO Ansgar Hinz apply].

17 November 2024. In the middle of the night. Deep down in the freezing, dark waters of the Baltic Sea, something happens that will shock Europe the following morning. Two of our continent's most important maritime data cables are severed within a matter of hours. The C-Lion1 cable between Finland and Germany. And shortly afterwards, the BCS East-West cable between Lithuania and Sweden.

From one second to the next, the direct, physical flow of data between these key European nations collapses.

This was not an extract from a geopolitical thriller. This was our reality. A surgical cut into our continent's digital carotid artery. A severed cable is, on the surface, a technical incident. But what we saw down there on the seabed of the Baltic Sea was the start of a domino effect. When cables like these fail, it doesn't simply mean that a few Netflix series stutter. It means that financial clearing systems grind to a halt. That European logistics chains lose their bearings. That data synchronisation between governments and critical data centres is interrupted. If a central element fails, it triggers a cascade of effects.

That, ladies and gentlemen, is the immense vulnerability of our modern, hyper-connected civilisation. And that is precisely why I am standing here this evening.

And with that, a warm welcome to the VDE Summer Reception 2026 here in Brussels. There is no more fitting venue for today's topic than this city. Here, at the very heart of the European institutions, decisions are being made on how we will organise our security in the future. Here, it will be decided whether Europe becomes a technologically sovereign power – or whether we are reduced to the digital and infrastructural periphery of other major powers.

My name is Ansgar Hinz – Mr Jaeger, thank you for the kind introduction – and I am Chairman of the Board of Europe's largest technology organisation for electrical, digital and information technology, the VDE. Founded by Werner von Siemens, the VDE has now been acting as a neutral technology guide for society, business and politics for well over 130 years.

Back to our topic.

Our topic today is 'The Resilience Code'. That sounds like pure technology. But at its core, it is about something far more fundamental: it is about our ability to survive. It is about our ability to remain capable of acting as a free, democratic society.

When I look at Europe today as an engineer, I must unfortunately conclude that, from a geopolitical perspective, we are not a highly agile, dynamic tech start-up. At present, we are behaving more like a massive, extremely sluggish *legacy system* – an outdated old system.

Here in Brussels, we sit together in countless high-profile working groups and spend years debating the front-end design with great passion. We spend 500 pages arguing about the soft pastel shade the European ‘Return’ button should glow in and how to design the perfect GDPR-compliant tick box. That is important, no doubt about it. But whilst we’re discussing the design out front in the lobby, critical security alerts are popping up every second in the backend of our system. Why? Because someone has long since breached the poorly secured backdoor and is bypassing our firewalls.

We are vulnerable. And we are being tested at this very moment, whilst we sit here in this hall.

The reality of hybrid warfare: the silent stress test

We are witnessing massive cyber-attacks on European institutions, sabotage of our critical infrastructure, orchestrated disinformation campaigns and targeted disruptions to our supply chains.

Think of aviation in the Baltic states. For months on end, well into 2024 and 2025, we witnessed massive, coordinated GPS jamming there – that is, the deliberate disruption and manipulation of satellite navigation signals. Over 4,000 civilian flights in Sweden, Poland, Lithuania and Finland were temporarily without reliable GPS. Aircraft were forced to turn back; routes were closed. Rescue helicopters and the coastguard lost their signals.

This is the true face of hybrid warfare. It always remains deliberately, almost to the millimetre, below the threshold of a conventional military attack. No one sends tanks across the border. No one formally declares war. But the cumulative effect of these constant, gruelling stress tests is radically and irreversibly altering our European security landscape.

Another example? Just a few days ago, in August 2026, a massive cyberattack struck CEVA Logistics, one of Europe’s largest logistics providers. Eight major European distribution centres were targeted. Data was compromised, and hardware supply chains were disrupted. In Europe, we have spent decades optimising our supply chains around a single metric: absolute cost-efficiency. ‘Just in time’. The cheapest supply chain has won. Today we are learning the hard way: the cheapest supply chain is of absolutely no use to you if it collapses at the very first digital stress test.

And what is often Europe’s first reaction to such incidents? Whether it’s severed cables or jammed radar signals, we often hear European politicians say: *“Well, we must first wait for a sufficient amount of legally admissible evidence to establish exactly who owned this ship or this jammer before we can take truly decisive action.”*

Let’s be honest: if your company server is on fire, do you call the fire brigade? Or do you first commission a government expert to establish, in a manner that will stand up in court, the cause of the fire and who was responsible, before you activate the fire-extinguishing system?

For heaven’s sake, we must not wait until the final court ruling to finally take our own vulnerabilities seriously. The attacker mercilessly exploits our legal and regulatory meticulousness against us.

Cascades and mindsets: the two fronts of vulnerability

Our vulnerabilities lie where we have long failed to recognise them as matters of security policy: electricity grids, ports, railways, communications networks, and healthcare. Without electricity, communications networks do not function. Without networks, data centres collapse. Without data centres, logistics break down, and without logistics, hospitals come under pressure. These systems

are not separate from one another. They form a highly complex integrated system. And that is precisely why our defence must be conceived in systemic terms.

But the attack is not directed solely against physical fibre-optic cables or server farms. If our rail or logistics infrastructure is repeatedly disrupted by sabotage, something very dangerous arises: frustration and mistrust amongst European citizens. A sense of the state's inability to maintain control takes hold. And this is precisely how a purely technical vulnerability becomes a highly dangerous societal vulnerability. The attacker does not need to paralyse a country with weapons. It is entirely sufficient for people to start believing that the state no longer has its own infrastructure under control.

This brings me to what is perhaps the most insidious dimension of this conflict: the war in our minds. We are subjected to daily attacks through fake news, through armies of bots on social media, through extremely well-crafted deepfakes and artificially amplified narratives. The adversary's aim here is not at all for us all to suddenly adopt their political ideology. That would be far too labour-intensive. Their aim is much more minimalist and effective: it is enough if, in the end, simply no one in our society knows what is true any more. When trust in our media, in science and in political institutions erodes, our society becomes paralysed.

By definition, a democracy must be an 'open-source' project. It thrives on open exchange, transparency and accessibility. But open-source does not mean having no firewalls. A democracy must never be defenceless!

The radical shift in perspective: from security to resilience

How do we escape this spiral? We need a fundamental, intellectual shift in perspective. We must move away from traditional 'security' towards genuine 'resilience'.

What is the difference? There is no such thing as 100 per cent security in complex systems. Traditional security builds a wall and asks: *How do we prevent the hack? How do we stop the attack?* The problem is: any wall can eventually be breached.

Resilience takes a crucial step further. Resilience also asks: *What happens if the attacker is already inside?* How quickly can we detect an anomaly in the system? How long can we continue to operate whilst under heavy attack? And – most importantly – how extremely quickly can we reboot and restore the system?

That is the difference between a rigid tank that breaks and an immune system that adapts and heals. 'Security by Design' is a thing of the past. We urgently need 'Resilience by Design'. And this applies to: communications networks, data centres, medical technology and military systems. And it applies just as much to organisations and to us as a society.

And that, ladies and gentlemen, must be approached from a European perspective. Threats know no borders. When it comes to critical infrastructure, Europe must not be a patchwork of national vanities. Politically and in terms of infrastructure, we must function like a vast, distributed, redundant cloud network. If a network node in Eastern Europe is attacked, the West must absorb the load in a spirit of solidarity, automatically and in real time – and vice versa. Europe must not merely face threats together; it is imperative that Europe be resilient together!

Technological sovereignty – Europe's nervous system

But resilience is not just a question of attitude; it is a question of technological hardware. And this brings us to the heart of European sovereignty.

Let us talk about microelectronics. Microchips are the invisible nervous system of our modern society. Without semiconductors, there is no modern radar, no secure encrypted communication, no navigation, no modern medical technology and – in an emergency – no functioning drone defence.

Europe's share of global chip production has declined dramatically in recent decades. We have outsourced our nervous system. Technological sovereignty does not mean self-sufficiency – we cannot and do not wish to isolate ourselves from the global market. But sovereignty means *the ability to act*. It is imperative that Europe strengthens its critical capabilities in the design, manufacture, packaging and testing of high-end chips. We must not allow geopolitical tensions in the Asian region to lead immediately to a technological standstill in Europe.

This applies just as much to the technologies of the future: artificial intelligence, sensor technology, quantum computing, power electronics, autonomous systems and drone technology. All of these are cutting-edge technologies. And almost all of these developments are now 'dual-use'. This means they have a civilian purpose but can be deployed for military purposes in a fraction of a second. A drone that delivers parcels today could block airports tomorrow. An AI algorithm that optimises logistics today could steer disinformation campaigns tomorrow.

This is precisely why we need organisations that not only develop but also regulate. Organisations that assess risks with an iron fist, set open standards and establish ethical guidelines.

VDE Defence: Our response, our DNA

And this is precisely where the VDE comes into play. Since its foundation in 1893, the VDE has stood for technological knowledge, technical progress, order, safety and, above all, trust. Our historical mission has never been to simply allow technical innovations to happen naively. Our mission has always been to make them trustworthy and safe through rules, rigorous testing and standards.

That is why, for us, the shift from 'safety' to 'resilience' is not a departure from our VDE DNA. It is its consistent, logical evolution into the 21st century. In the past, we prevented faults in individual components. Today, we make complex, integrated systems resilient under fire.

To tackle this, we have opened a completely new chapter. We have launched **VDE Defense** on the basis of our existing comprehensive expert knowledge. Why? Because we are deeply convinced that a country's civil security and defence capability today no longer depend solely on generals and the armed forces. They depend heavily on engineers who design more robust systems, cut dependencies and harden our infrastructure.

VDE Defense focuses on five key areas:

Firstly: resilience. Infrastructure – from hardware components to the European cloud – must be able to withstand disruptions.

Secondly: technological sovereignty. The aforementioned capacity to act in the fields of microelectronics and semiconductors.

Thirdly: research and new technologies. The responsible use of dual-use technologies, AI and quantum computing.

Fourthly: people and skilled workers. We can import chips and software. But we cannot conjure up talented minds out of thin air. Without excellent engineers, there can be no cybersecurity and no resilience. Securing a skilled workforce has long since become a hard-hitting aspect of European security policy.

Fifthly: testing, certification and trust. Technology alone does not create trust. Trust is built through independent, verifiable transparency. We must be able to demonstrate, even under extreme stress tests, that what we consider to be fail-safe actually is.

Such a milestone does not come about by itself. It is created by visionary minds who bring together technology, industry, science and politics around one table. My very special thanks today therefore also go to Markus B. Jaeger and his brilliant team. They work tirelessly to ensure that the VDE's voice is heard where political and strategic decisions are made: in Germany, in Europe and internationally. Markus B. Jaeger heads VDE Defence – and as a lieutenant-colonel in the reserves, an experienced lawyer and a political strategist, he is virtually predestined for this role at the interface of these fields.

To the next generation: Ethics by Design as the ultimate hack

This brings me to you. Here in this hall this evening, I see so many young faces. I see the talented individuals, developers, tech strategists and young professionals. To the generation that will hold the future of this Europe in their hands over the coming decades.

At conferences like this, you often hear people of my generation utter this one, fatherly phrase: *“We’ll soon be passing the baton on to you.”*

You know what? Forget the baton. That’s the wrong metaphor. We simply have no time left for ceremonial handovers in the future. We need you *now*, this evening, first thing tomorrow morning, at our tables.

My generation has learnt to think in clear-cut silos, rigid hierarchies and isolated individual components. That has taken us a long way. But the world has moved on. You? You think natively in networks, in APIs, in decentralised systems and global open-source communities. You intuitively understand how cascade effects work, because you’ve grown up with them.

Technology is never neutral. It is dual-use. And in today’s geopolitical reality, building resilience is not a tedious, bureaucratic compliance issue. Embedding genuine resilience and *Ethics by Design* into digital systems is the ultimate intellectual engineering challenge of our time!

Don’t let anyone convince you that you are merely executors. If you are designing network architectures in Europe today, if you are designing hardware, if you are training AI models or writing code, then you are not simply doing a tech job.

At this very moment, you are shaping tangible European security policy! With every line of code, with every encrypted API, you are building the digital architecture of our European freedom. Take ownership of this space. Fill it with your ideas. Be radical in your thinking and pragmatic in your actions.

Ladies and gentlemen, we must face up to the bitter reality: our adversaries will continue to test our vulnerabilities, every day, every hour. The question we must ask ourselves is no longer: *Will we be attacked?* The question is, and has long been: **How resilient are we when it happens?**

We must not wait until the next cable break, the next blackout or the next major cyber incident painfully reveals where our weaknesses lie. We must identify these weaknesses now; we must measure them ruthlessly and reduce them drastically. To do this, we need technological excellence, but technology alone is not enough. We need a holistic approach.

That is why, to conclude, I am today making three clear appeals to the key players here in this room and across Europe:

Firstly, to policymakers: Say goodbye to the old, legacy way of thinking! We cannot design European security for the 21st century on the drawing board in endless committees whilst our systems

are burning outside. We need speed. We need pragmatic European cooperation, rapid funding for critical infrastructure and common, open standards instead of national self-interest and bureaucratic behemoths. Create the regulatory framework that will finally make us agile and resilient!

Secondly, to business and industry: Stop blindly prioritising radical financial efficiency above all else. Stop optimising down to the last decimal place if it means sacrificing your stability. Technological sovereignty and resilience cost money – but they are our European life insurance. ‘Resilience by Design’ must be integrated into every development department, every infrastructure plan and every new data centre with immediate effect. Make our systems resilient from the ground up!

And thirdly, to our society: A democracy can only withstand as much as its citizens are prepared to defend it. Do not allow disinformation, deepfakes and toxic algorithms to erode our social cohesion from within. Remain critical. Question narratives. Understand that an open society can only survive if it is defiant and resilient in spirit!

The great scholar Wilhelm von Humboldt once coined the wise phrase: *“Without security, there is no freedom.”*

Today, in the age of hybrid attacks and asymmetric warfare, we must urgently expand on this phrase. We must say: *“Without resilience, security is not sustainable.”*

Our goal is not a utopian world without risks, without mistakes or without crises. That is an illusion. Our great European goal is a society that recognises risks at an early stage; that confidently fends off hybrid attacks; that can withstand even severe infrastructural disruptions; that recovers at breakneck speed; and that, under maximum pressure, remains exactly what defines it at its core: free, self-determined and unwaveringly democratic.

That is our task.

That is the Resilience Code. And Europe must start writing it. Now.

Thank you very much!

Markus B. Jaeger

VDE Verband der Elektrotechnik
Elektronik Informationstechnik e.V.
Bismarckstr. 33
10625 Berlin
Mobil: +49 171 7631986
Markusb.jaeger@vde.com