



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

[Es gilt das gesprochene Wort von VDE CEO Ansgar Hinz]

17. November 2024. Mitten in der Nacht. Tief unten, im eiskalten und dunklen Wasser der Ostsee, passiert etwas, das Europa am nächsten Morgen schockieren wird. Zwei der wichtigsten maritimen Datenkabel unseres Kontinents werden innerhalb weniger Stunden durchtrennt. Das C-Lion1-Kabel zwischen Finnland und Deutschland. Und kurz darauf das BCS East-West-Kabel zwischen Litauen und Schweden.

Von einer Sekunde auf die andere bricht der direkte, physische Datenstrom zwischen diesen europäischen Kernländern zusammen.

Das war kein Auszug aus einem geopolitischen Thriller. Das war unsere Realität. Ein chirurgischer Schnitt in die digitale Halsschlagader unseres Kontinents. Ein durchtrenntes Kabel ist vordergründig ein technisches Ereignis. Aber was wir dort unten auf dem Meeresgrund der Ostsee gesehen haben, war der Beginn eines Dominoeffekts. Wenn solche Kabel ausfallen, bedeutet das nicht einfach nur, dass ein paar Netflix-Serien ruckeln. Es bedeutet, dass Finanzclearing-Systeme ins Stocken geraten. Dass europäische Logistik-Ketten die Orientierung verlieren. Dass die Datensynchronisation zwischen Regierungen und kritischen Rechenzentren unterbrochen wird. Fällt ein zentrales Element aus, entstehen Kaskadeneffekte.

Das, meine Damen und Herren, ist die immense Verwundbarkeit unserer modernen, hyper-vernetzten Zivilisation. Und genau deshalb stehe ich heute Abend hier.

Und damit herzlich willkommen zur VDE Summer Reception 2026 hier in Brüssel. Es gibt keinen passenderen Ort für unser heutiges Thema als diese Stadt. Hier, in den Herzkammern der europäischen Institutionen, entscheidet sich, wie wir in Zukunft unsere Sicherheit organisieren. Hier entscheidet sich, ob Europa eine technologisch souveräne Macht wird – oder ob wir zur digitalen und infrastrukturellen Peripherie anderer Großmächte verkommen.

Mein Name ist Ansgar Hinz – Herr Jaeger, danke für die freundliche Vorstellung – und ich bin Chairman of the Board von Europas größter Technologieorganisation der Elektro-, Digital- und Informationstechnik, dem VDE. Gegründet durch Werner von Siemens wirkt der VDE nun seit weiter über 130 Jahren als neutraler Technologie-Navigator für Gesellschaft, Wirtschaft und Politik.

Zurück zu unserem Thema.

Unser Titel heute lautet „The Resilience Code“. Das klingt nach reiner Technologie. Aber im Kern geht es um etwas sehr viel Grundlegenderes: Es geht um unsere Überlebensfähigkeit. Es geht um unsere Fähigkeit, als freie, demokratische Gesellschaft handlungsfähig zu bleiben.

Wenn ich mir Europa heute als Ingenieur anschau, dann muss ich leider feststellen: Wir sind geopolitisch gesehen kein hochagiles, dynamisches Tech-Start-up. Wir verhalten uns aktuell eher wie ein massives, extrem träges *Legacy-System* – ein veraltetes Alt-System.

Wir sitzen hier in Brüssel in zahllosen, hochkarätig besetzten Arbeitsgruppen zusammen und debattieren jahrelang leidenschaftlich über das Frontend-Design. Wir streiten auf 500 Seiten darüber, in welchem sanften Pastellton der europäische "Return"-Button leuchten soll und wie wir die perfekte DSGVO-konforme Checkbox designen. Das ist wichtig, zweifellos. Aber während wir vorne in der Lobby über das Design diskutieren, schlagen im Backend unseres Systems im Sekundentakt die kritischen Security-Warnungen auf. Warum? Weil längst jemand durch die schlecht gesicherte Hintertür eingedrungen ist und unsere Firewalls umgeht.

Wir sind verwundbar. Und wir werden genau in diesem Moment, während wir hier im Saal sitzen, getestet.

Die Realität der hybriden Kriegsführung: Der lautlose Stresstest

Wir sehen massive Cyberangriffe auf europäische Institutionen, Sabotage an unserer kritischen Infrastruktur, orchestrierte Desinformationskampagnen und gezielte Störungen unserer Logistikketten.

Denken Sie an die Luftfahrt im Baltikum. Über Monate hinweg, bis tief in die Jahre 2024 und 2025 hinein, erlebten wir dort ein massives, koordiniertes GPS-Jamming – also das gezielte Stören und Manipulieren von Satellitennavigationssignalen. Über 4.000 Zivilflüge in Schweden, Polen, Litauen und Finnland waren zeitweise ohne verlässliches GPS. Flugzeuge mussten umkehren, Routen wurden gesperrt. Rettungshubschrauber und die Küstenwache verloren ihre Signale.

Das ist die wahre Fratze der hybriden Kriegsführung. Sie bleibt immer bewusst, fast schon millimetergenau, unterhalb der Schwelle eines klassischen militärischen Angriffs. Niemand schickt Panzer über die Grenze. Niemand erklärt formell den Krieg. Aber die Summe dieser ständigen, zermürenden Stresstests verändert unsere europäische Sicherheitslage radikal und unumkehrbar.

Ein weiteres Beispiel? Erst vor wenigen Tagen, im August 2026, traf ein massiver Cyberangriff CEVA Logistics, einen der größten Logistik-Dienstleister in Europa. Acht große europäische Verteilzentren wurden attackiert. Daten wurden kompromittiert, Hardware-Lieferketten gestört. Wir haben in Europa unsere Supply Chains jahrzehntelang auf eine einzige Metrik hin optimiert: absolute Kosteneffizienz. "Just in time". Die billigste Lieferkette hat gewonnen. Heute lernen wir auf die harte Tour: Die billigste Lieferkette nützt Ihnen rein gar nichts, wenn sie beim allerersten digitalen Stresstest in sich zusammenfällt.

Und was ist oft Europas erste Reaktion auf solche Vorfälle? Egal ob es um zerschnittene Kabel oder blockierte Radarsignale geht, oft hören wir aus der europäischen Politik den Satz: *„Nun ja, wir müssen erst eine ausreichende Anzahl an gerichtsfesten juristischen Beweis abwarten, wem genau dieses Schiff oder dieser Störsender gehörte, bevor wir wirklich konsequent handeln können.“*

Mal ehrlich: Wenn Ihr Unternehmensserver brennt, rufen Sie dann die Feuerwehr? Oder beauftragen Sie erst einen staatlichen Gutachter, der gerichtsfest die Brandursache und die Urheberschaft klärt, bevor Sie die Löschanlage aktivieren?

Wir dürfen um Himmels willen nicht warten, bis das letzte Gericht entscheidet, um unsere eigenen Verwundbarkeiten endlich ernst zu nehmen. Der Angreifer nutzt unsere rechtliche und regulatorische Akribie gnadenlos gegen uns aus.

Kaskaden und Köpfe: Die zwei Fronten der Verwundbarkeit

Unsere Verwundbarkeiten liegen dort, wo wir sie lange nicht als Sicherheitspolitik verstanden haben: Stromnetze, Häfen, Eisenbahnen, Kommunikationsnetze, Medizinische Versorgung. Ohne Strom funktionieren keine Kommunikationsnetze. Ohne Netze kollabieren Rechenzentren. Ohne Rechenzentren fällt die Logistik aus, und ohne Logistik geraten Krankenhäuser unter Druck. Diese Systeme sind nicht voneinander getrennt. Sie bilden ein hochkomplexes Gesamtsystem. Und genau deshalb muss unsere Verteidigung systemisch gedacht werden.

Aber der Angriff richtet sich nicht nur gegen physische Glasfaserkabel oder Serverfarmen. Wenn unsere Bahn- oder Logistik-Infrastruktur durch Sabotage immer wieder gestört wird, entsteht etwas sehr Gefährliches: Frustration und Misstrauen bei den europäischen Bürgern. Ein Gefühl staatlicher Kontrolllosigkeit macht sich breit. Und exakt so wird aus einer rein technischen Verwundbarkeit eine hochgefährliche gesellschaftliche Verwundbarkeit. Der Angreifer muss ein Land nicht mit Waffen lahmlegen. Es reicht völlig, wenn die Menschen beginnen zu glauben, dass der Staat seine eigene Infrastruktur nicht mehr im Griff hat.

Das bringt mich zur vielleicht perfidesten Dimension dieses Konflikts: Der Krieg in unseren Köpfen. Wir erleben den täglichen Angriff durch Fake News, durch Bot-Armeen auf Social Media, durch extrem gut gemachte Deepfakes und künstlich verstärkte Narrative. Das Ziel des Gegners dabei ist gar nicht, dass wir alle plötzlich seine politische Ideologie übernehmen. Das wäre viel zu aufwendig. Sein Ziel ist viel minimalistischer und effektiver: Es reicht, wenn am Ende in unserer Gesellschaft einfach niemand mehr weiß, was wahr ist. Wenn das Vertrauen in unsere Medien, in die Wissenschaft, in politische Institutionen erodiert, wird unsere Gesellschaft handlungsunfähig.

Eine Demokratie muss per Definition ein "Open-Source"-Projekt sein. Sie lebt vom offenen Austausch, von Transparenz und Zugänglichkeit. Aber Open-Source bedeutet nicht, dass man keine Firewalls hat. Eine Demokratie darf niemals wehrlos sein!

Der radikale Perspektivwechsel: Von Security zu Resilience

Wie entkommen wir aus dieser Spirale? Wir brauchen einen fundamentalen, intellektuellen Perspektivwechsel. Wir müssen den Weg gehen von klassischer "Security" hin zu echter "Resilience".

Wo liegt der Unterschied? 100 Prozent Sicherheit gibt es in komplexen Systemen nicht. Klassische Sicherheit, "Security", zieht eine Mauer hoch und fragt: *Wie verhindern wir den Hack? Wie stoppen wir den Angriff?* Das Problem ist: Jede Mauer kann irgendwann überwunden werden.

Resilienz geht einen entscheidenden Schritt weiter. Resilienz fragt zusätzlich: *Was passiert, wenn der Gegner drin ist?* Wie schnell erkennen wir die Anomalie im System? Wie lange können wir unter massivem Beschuss weiterarbeiten? Und – am wichtigsten – wie extrem schnell können wir das System neu booten und wiederherstellen?

Das ist der Unterschied zwischen einem starren Panzer, der bricht, und einem Immunsystem, das sich anpasst und heilt. „Security by Design“ war gestern. Wir brauchen zwingend „Resilience by Design“. Und das gilt für: Kommunikationsnetze, Rechenzentren, Medizintechnik, militärische Systeme. Und es gilt genauso für Organisationen und für uns als Gesellschaft.

Und das, meine Damen und Herren, muss europäisch gedacht werden. Bedrohungen kennen keine Grenzen. Europa darf in kritischen Infrastrukturen kein Flickenteppich aus nationalen Eitelkeiten sein. Wir müssen politisch und infrastrukturell funktionieren wie ein riesiges, verteiltes, redundantes Cloud-Netzwerk. Wenn ein Netzknoten im Osten Europas attackiert wird, muss der Westen die Last solidarisch, automatisiert und in Echtzeit abfedern – und umgekehrt. Europa darf nicht nur gemeinsam bedroht sein, Europa muss zwingend gemeinsam resilient sein!

Technologische Souveränität – Das Nervensystem Europas

Aber Resilienz ist nicht nur eine Frage der Haltung, sie ist eine Frage der technologischen Hardware. Und hier kommen wir zum Kern europäischer Souveränität.

Lassen Sie uns über Mikroelektronik sprechen. Mikrochips sind das unsichtbare Nervensystem unserer modernen Gesellschaft. Ohne Halbleiter gibt es kein modernes Radar, keine sichere verschlüsselte Kommunikation, keine Navigation, keine moderne Medizintechnik und – im Ernstfall – keine funktionierende Drohnenabwehr.

Der europäische Anteil an der weltweiten Chipproduktion ist in den letzten Jahrzehnten dramatisch zurückgegangen. Wir haben unser Nervensystem ausgelagert. Technologische Souveränität bedeutet nicht Autarkie – wir können und wollen uns nicht vom Weltmarkt abschotten. Aber Souveränität bedeutet *Handlungsfähigkeit*. Europa muss zwingend kritische Kompetenzen im Design, in der Fertigung, im Packaging und in der Prüfung von High-End-Chips stärken. Wir dürfen nicht zulassen, dass geopolitische Spannungen im asiatischen Raum sofort zu einem technologischen Herzstillstand in Europa führen.

Das gilt genauso für die Technologien der Zukunft: Künstliche Intelligenz, Sensorik, Quantencomputing, Leistungselektronik, autonome Systeme und Drohnentechnologie. All das ist Hochtechnologie. Und fast all diese Entwicklungen sind heute „Dual Use“. Das bedeutet, sie haben einen zivilen Nutzen, lassen sich aber in Sekundenbruchteilen militärisch einsetzen. Eine Drohne, die heute Pakete ausliefert, kann morgen Flughäfen blockieren. Ein KI-Algorithmus, der heute die Logistik optimiert, kann morgen Desinformationskampagnen steuern.

Genau deshalb braucht es Organisationen, die nicht nur entwickeln, sondern ordnen. Die Risiken knallhart bewerten, offene Standards setzen und ethische Leitplanken einziehen.

VDE Defense: Unsere Antwort, unsere DNA

Und exakt hier kommt der VDE ins Spiel. Der VDE steht seit seiner Gründung im Jahr 1893 für technologisches Wissen, technischen Fortschritt, Ordnung, Sicherheit und vor allem: Vertrauen. Unsere historische Aufgabe war es nie, technische Innovationen einfach naiv geschehen zu lassen. Unsere Aufgabe war es immer, sie durch Regeln, knallharte Prüfungen und Standards vertrauenswürdig und sicher zu machen.

Deshalb ist der Schritt von "Sicherheit" zu "Resilienz" für uns keine Abkehr von unserer VDE-DNA. Es ist ihre konsequente, logische Weiterentwicklung im 21. Jahrhundert. Früher haben wir Fehler in Einzelkomponenten vermieden. Heute machen wir komplexe Gesamtsysteme unter Feuer resilient.

Um das zu stemmen, haben wir ein völlig neues Kapitel aufgeschlagen. Wir haben **VDE Defense** auf Basis unseres schon vorhandenen umfassenden Expertenwissens ins Leben gerufen. Warum? Weil wir der tiefen Überzeugung sind, dass die zivile Sicherheit und die Verteidigungsfähigkeit eines Landes heute eben nicht mehr allein von Generälen und Streitkräften abhängen. Sie hängen massiv von Ingenieurinnen und Ingenieuren ab, die Systeme robuster gestalten, Abhängigkeiten kappen und unsere Infrastruktur härten.

VDE Defense fokussiert sich auf fünf elementare Schwerpunkte:

Erstens: Resilienz. Infrastrukturen, von der Hardware-Komponente bis zur europäischen Cloud, müssen Störungen verkraften.

Zweitens: Technologische Souveränität. Die angesprochene Handlungsfähigkeit bei Mikroelektronik und Halbleitern.

Drittens: Forschung und neue Technologien. Der verantwortungsvolle Umgang mit Dual-Use-Technologien, KI und Quanten.

Viertens: Menschen und Fachkräfte. Wir können Chips und Software importieren. Aber wir können keine talentierten Köpfe herbeizaubern. Ohne exzellente Ingenieure gibt es keine Cybersecurity und keine Resilienz. Fachkräftesicherung ist längst knallharte europäische Sicherheitspolitik geworden.

Fünftens: Prüfung, Zertifizierung und Vertrauen. Technologie allein schafft kein Vertrauen. Vertrauen entsteht durch unabhängige, überprüfbare Transparenz. Was wir für ausfallsicher halten, müssen wir unter extremen Stresstests auch nachweisen können.

Ein solcher Meilenstein entsteht nicht von selbst. Er entsteht durch visionäre Köpfe, die Technologie, Industrie, Wissenschaft und Politik an einen Tisch zwingen. Mein ganz besonderer Dank gilt daher heute auch Markus B. Jaeger und seinem brillanten Team. Sie sorgen unermüdlich dafür, dass die Stimme des VDE dort gehört wird, wo politische und strategische Entscheidungen fallen: in Deutschland, in Europa und international. Markus B. Jaeger leitet VDE Defense – und als Oberstleutnant der Reserve, als erfahrener Jurist und politischer Kopf ist er für diese Schnittstellenaufgabe geradezu prädestiniert.

An die Next Generation: Ethics by Design als ultimativer Hack

Damit bin ich bei Ihnen. Ich blicke heute Abend hier im Saal in sehr viele junge Gesichter. Auf die Talente, Entwickler, Tech-Strategen und Young Professionals. Auf die Generation, die dieses Europa in den nächsten Jahrzehnten in ihren Händen halten wird.

Auf Konferenzen wie dieser hört man von Leuten meiner Generation oft diesen einen, väterlichen Satz: *"Wir übergeben euch bald den Staffelstab."*

Wissen Sie was? Vergessen Sie den Staffelstab. Das Bild ist falsch. Wir haben absolut keine Zeit mehr für feierliche Übergaben in der Zukunft. Wir brauchen Sie *jetzt*, heute Abend, morgen früh an unseren Tischen.

Meine Generation hat gelernt, in klaren Silos, in starren Hierarchien und isolierten Einzelkomponenten zu denken. Das hat uns weit gebracht. Aber die Welt hat sich gedreht. Sie? Sie denken nativ in Netzwerken, in APIs, in dezentralen Systemen und globalen Open-Source-Communities. Sie verstehen intuitiv, wie Kaskadeneffekte funktionieren, weil Sie mit ihnen aufgewachsen sind.

Technologie ist niemals neutral. Sie ist Dual Use. Und in der heutigen geopolitischen Realität ist der Aufbau von Resilienz kein lästiges, bürokratisches Compliance-Thema. Echte Resilienz und *Ethics by Design* in digitale Systeme zu gießen, ist die ultimative, intellektuelle Ingenieurs-Herausforderung unserer Zeit!

Lassen Sie sich nicht einreden, Sie seien nur Ausführende. Wenn Sie heute in Europa Netzwerkarchitekturen entwerfen, wenn Sie Hardware designen, wenn Sie KI-Modelle trainieren oder Code schreiben, dann machen Sie nicht einfach nur einen Tech-Job.

Sie schreiben in diesem Moment handfeste europäische Sicherheitspolitik! Mit jeder Zeile Code, mit jeder verschlüsselten API bauen Sie die digitale Architektur unserer europäischen Freiheit. Übernehmen Sie diesen Raum. Füllen Sie ihn mit Ihren Ideen. Seien Sie radikal im Denken und pragmatisch im Handeln.

Meine Damen und Herren, wir müssen der bitteren Realität ins Auge sehen: Unsere Gegner werden unsere Verwundbarkeiten weiter testen, jeden Tag, jede Stunde. Die Frage, die wir uns stellen müssen, lautet schon lange nicht mehr: *Werden wir angegriffen?* Die Frage lautet einzig und allein: **Wie resilient sind wir, wenn es passiert?**

Wir dürfen nicht warten, bis der nächste Kabelriss, der nächste Blackout oder der nächste große Cyber-Vorfall uns schmerzhaft offenbart, wo unsere Schwächen liegen. Wir müssen diese Schwächen jetzt kennen, wir müssen sie gnadenlos messen und drastisch reduzieren. Dafür brauchen wir technologische Exzellenz, aber Technologie allein reicht nicht. Wir brauchen einen holistischen Ansatz.

Deshalb richte ich heute zum Abschluss drei klare Appelle an die entscheidenden Akteure hier im Raum und in Europa:

Erstens, an die Politik: Verabschieden Sie sich vom alten Legacy-Denken! Wir können europäische Sicherheit im 21. Jahrhundert nicht in endlosen Gremien auf dem Reißbrett entwerfen, während draußen unsere Systeme brennen. Wir brauchen Geschwindigkeit. Wir brauchen pragmatische europäische Zusammenarbeit, schnelle Budgets für kritische Infrastruktur und gemeinsame, offene Standards anstelle von nationalen Egoismen und Bürokratie-Monstern. Schaffen Sie den regulatorischen Rahmen, der uns endlich agil und wehrhaft macht!

Zweitens, an die Wirtschaft und die Industrie: Hören Sie auf, radikale finanzielle Effizienz blind über alles zu stellen. Optimieren Sie nicht länger auf die letzte Nachkommastelle, wenn Sie dafür Ihre Stabilität opfern. Technologische Souveränität und Resilienz kosten Geld – aber sie sind unsere europäische Lebensversicherung. „Resilience by Design“ muss ab sofort in jede Entwicklungsabteilung, in jede Infrastrukturplanung und in jedes neue Rechenzentrum integriert werden. Machen Sie unsere Systeme von Grund auf widerstandsfähig!

Und drittens, an unsere Gesellschaft: Eine Demokratie hält immer nur so viel aus, wie ihre Bürgerinnen und Bürger bereit sind zu verteidigen. Lassen Sie nicht zu, dass Desinformation, Deepfakes und toxische Algorithmen unseren gesellschaftlichen Zusammenhalt von innen heraus zersetzen. Bleiben Sie kritisch. Hinterfragen Sie Narrative. Verstehen Sie, dass eine offene Gesellschaft nur überleben kann, wenn sie wehrhaft und resilient im Geiste ist!

Der große Gelehrte Wilhelm von Humboldt hat einmal den klugen Satz geprägt: *„Ohne Sicherheit ist keine Freiheit.“*

Heute, im Zeitalter der hybriden Angriffe und der asymmetrischen Kriegsführung, müssen wir diesen Satz zwingend erweitern. Wir müssen sagen: *„Ohne Resilienz ist Sicherheit nicht dauerhaft.“*

Unser Ziel ist keine utopische Welt ohne Risiken, ohne Fehler oder ohne Krisen. Das ist eine Illusion. Unser großes europäisches Ziel ist eine Gesellschaft, die Risiken früh erkennt. Die hybride Angriffe souverän abwehrt. Die selbst schwere infrastrukturelle Störungen verkraftet. Die sich rasend schnell erholt und die unter maximalem Druck genau das bleibt, was sie im Kern ausmacht: Frei, selbstbestimmt und unerschütterlich demokratisch.

Das ist unsere Aufgabe.

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

Vielen Dank!

Markus B. Jaeger

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