The New Realities of Digital Geopolitics

Background reading for the SCION Day 2026 keynote

This is a long piece, and there's a reason for that. The talk I'm giving at SCION Day 2026 is twenty minutes, which simply isn't enough time to walk through the evidence behind any of the claims I'll make on stage. So what follows is the dossier behind the talk — the primary sources, the dates, the procedural detail, and the reasoning that connects one piece of evidence to the next. I've written it for myself first, so I can stand in front of the room with the full record in mind even when I'm only quoting a fragment of it. I've also written it so that the people in the room can verify any of the load-bearing claims afterwards, link by link, in their own time.
The thesis is straightforward. The contest we used to call 'cyber security' has become indistinguishable from the broader contest over the international order. And the principal players in that international order — the Russian Federation, the People's Republic of China, and the United States of America — have over the past eighteen months made their respective positions unmistakable in operational terms. They've done it through actions rather than statements; the statements, where they exist, are mostly attempts to explain or to deny what's already happened in practice. The European Union finds itself responding to all three, with instruments that didn't exist eighteen months ago and a vocabulary that's still being assembled in real time.

The Dutch position, which is what concerns me most directly, is harder than it looks. The Netherlands is simultaneously a target of Russian sabotage and espionage, a target of Chinese strategic intelligence collection, and a customer of the American digital stack at a moment when the legal architecture underlying that stack has been quietly weaponized. The combination isn't unique to us — Germany, France, Italy and Belgium all sit in roughly the same position — but the Dutch case is unusually well documented, because our intelligence services have chosen, over the past three years, to publish more than they used to. The AIVD's annual report of 2025, published on 23 April 2026, and the MIVD's annual report of 2025, published on 21 April 2026, are remarkable documents. They're also where I'll end this piece.

The structure is as follows. I'll begin with the Russian vector, because that's where the story sits most visibly in the public mind, and because the doctrinal foundations go back the furthest. Then I'll turn to the Chinese vector, which operates at a different scale and against a different layer of the stack. After that, the American vector — the legal architecture, the events that turned it from theoretical to operational, and the institutional responses on both sides of the Atlantic. I'll close with the European response, the framework that now sits underneath it, and the observation I'll end the talk on.

I. The Russian Vector

Doctrinal foundations

It's tempting to read the Russian campaign of the past three years as a response to the war in Ukraine — and there's no doubt that the invasion of February 2022 and the subsequent reorientation of European policy towards Russia provided both opportunity and incentive for what we now see. But the doctrinal architecture is a great deal older than that. The classic reference point is Colonel Vitaly Tsymbal's 1995 article in Voennaya Mysl, the Russian general staff journal, in which Tsymbal argued that cyber attacks could function as a substitute for nuclear deterrence — cheaper, more deniable, and easier to calibrate against a wider range of adversaries. The piece is unusual not for its predictions, which mostly turned out to be right, but for its candor about what cyber operations were being designed to do: not protect networks, but project state power.

Eighteen years later, in February 2013, Russia's then Chief of the General Staff Valery Gerasimov published the article in *Voenno-Promyshlennyi Kurier* that would become known in the West as the 'Gerasimov Doctrine'. The Western label is somewhat misleading — Gerasimov's article is largely descriptive rather than prescriptive, and the term 'doctrine' was attached to it by Western analysts rather than by Russian military theorists themselves. But the substance is real. Gerasimov's central claim was that non-military means had come to play a decisive role in achieving strategic objectives — in many cases, he argued, surpassing the effectiveness of conventional military force — and that the integration of those non-military means with traditional military instruments would define the contests of the coming decades.

What I want to extract from that doctrinal background is a single observation: the Russian campaign we now see is not an improvisation. It's the operational realization of a way of thinking that's been documented in Russian military journals for thirty years. The fact that the West chose not to take that thinking seriously until relatively recently is on the West, not on the Russians.

The Baltic shadow fleet

The publicly visible face of the Russian campaign over the past two years has been the systematic damaging of undersea cables in the Baltic Sea by ships flagged outside the European Union. The list is now long enough to be worth setting out chronologically. In October 2023, a Chinese-flagged cargo vessel called *Newnew Polar Bear* damaged the Balticconnector gas pipeline between Finland and Estonia, along with two adjacent data cables. The Chinese government declined to cooperate with the Finnish investigation. In November 2024, another Chinese-flagged vessel, *Yi Peng 3*, severed the C-Lion 1 cable between Finland and Germany and the BCS East-West Interlink between Lithuania and Sweden. Sweden requested permission to conduct an investigation on the ship; China refused; the ship eventually left the area.

On 25 December 2024 came *Eagle S* — the case I lead with on stage, because the documentary record is unusually complete. The vessel is Cook Islands-flagged, but the Cook Islands shipping registry is administered by Maritime Cook Islands, a private corporation operating under a delegated mandate from the Cook Islands government. The vessel's registered owner is Caravella LLC FZ, a United Arab Emirates free-zone company. Its commercial operator is Peninsular Maritime, an Indian firm. Its cargo on the relevant voyage was unleaded petrol loaded at Ust-Luga, a Russian Baltic port, bound for Port Said in Egypt. The Finnish authorities have publicly stated that the vessel is part of the Russian 'shadow fleet' — the term of art for tankers that ship Russian oil in defiance of the G7/EU/Australian sanctions regime, generally under obscure ownership and without Western-regulated insurance.

The damage was extensive. The Estlink-2 power cable between Finland and Estonia went down at approximately 12:26 local time on Christmas Day. Four data cables along the same corridor were damaged in the same sequence of hours. Finnish investigators subsequently established that the vessel had dragged its anchor across the seabed for approximately ninety kilometers, leaving a continuous gouge visible on subsea survey. Finnish authorities boarded the vessel on 26 December and detained its officers. The cargo was held by Finnish Customs on the grounds that it likely contravened sanctions.

Here's where the legal architecture of deniability becomes most clearly visible. On 3 October 2025, the Helsinki District Court ruled it didn't have criminal jurisdiction over the officers of the vessel, on the basis of Article 97(1) of the United Nations Convention on the Law of the Sea, which reserves criminal jurisdiction over

a ship to its flag state. The flag state is the Cook Islands. The Cook Islands have a population of approximately seventeen thousand and no functioning maritime court. The case won't be tried.

It's worth being precise about what this means. UNCLOS Article 97 was drafted with collisions and accidental damage in mind, not with the systematic instrumentalization of flag-of-convenience registries by a state actor. The drafters couldn't, in 1982, have anticipated that an oil-importing power would acquire a fleet of obscurely-owned tankers, register them under jurisdictions chosen for their evaporative qualities, and use them to drag anchors across critical infrastructure as part of a coordinated campaign. The instrument hasn't been amended; the loophole has been weaponized. There is, as I write this in May 2026, no agreed European or NATO response, although the alliance has established a permanent Baltic Sentry mission and the EU has imposed additional sanctions on individual shadow-fleet vessels.

After Eagle S came two further incidents: Fitburg in December 2025, and the Sventoji-Liepāja cable damage in January 2026. By the time of writing, the public record contains at least seven Baltic cable incidents linked to vessels with Russian or Chinese connections in the eighteen months between November 2024 and January 2026. NATO's response has been Baltic Sentry, a multinational maritime surveillance operation launched in January 2025 and made permanent in subsequent communiqués. The mission monitors traffic patterns and is empowered to board vessels suspected of involvement, but the operational reality remains that boarding a vessel doesn't, on its own, alter the underlying jurisdictional problem.

Laundry Bear

On 27 May 2025, the AIVD and the MIVD jointly disclosed an intrusion against the Dutch National Police that had begun in September 2024. They named the actor Laundry Bear. The operation extracted the work contact details — names, telephone numbers, work email addresses, and in some cases physical office locations — of essentially the entire Dutch National Police force. The public assessment was that the actor was Russian state-sponsored, distinct from the well-known GRU-affiliated APT28 and the SVR-affiliated APT29, and previously unknown to Western intelligence services.

The decision to disclose is itself worth dwelling on. Intelligence services don't routinely attribute breaches in public; they do so when the operational benefit of disclosure outweighs the cost of revealing what they know. In this case the calculation appears to have been that the scale of the intrusion, the sensitivity of the data, and the fact that the same actor was likely operating elsewhere in Europe made disclosure the responsible course. Subsequent reporting by Microsoft Threat Intelligence linked the same actor to intrusions against European NATO members' government infrastructure and against critical infrastructure operators across the continent. Microsoft's threat intelligence team designates the actor as Void Blizzard; the Dutch services use the Laundry Bear designation; the underlying capability appears to be the same.

What does this tell us about the Russian campaign? Two things. First, that the operational tempo hasn't slackened with the failure of the Ukrainian counteroffensive or the various ceasefire proposals; if anything, the espionage thread has accelerated. Second, that the universe of named Russian actors continues to expand. The pattern of 'previously unknown' actors emerging in public disclosures suggests there's a deeper bench of operational capabilities than Western intelligence services had previously assessed, and that the visible part of Russian state-sponsored cyber activity is only the part that's been caught.

Voice of Europe

The influence thread is the least technical of the three, and in some ways the most disturbing, because it operates inside the institutions of European democracy rather than against them from the outside. The *Voice of Europe* case is now well documented. The website *voiceofeurope.com* was originally founded in the Netherlands in 2016 by a Dutch businessman named Erik de Vlieger. It published right-leaning commentary in English and ran for several years before being allowed to lapse in 2019. In 2023 it was revived under different ownership, operating out of Prague, and began publishing content critical of EU support for Ukraine and favorable to Russian positions.

On 27 March 2024, the Czech Security Information Service (BIS) issued a public statement confirming that the operation was being run by Viktor Medvedchuk — a former Ukrainian politician with personal ties to Putin who had been part of a prisoner exchange in September 2022 — through an intermediary named Artyom

Marchevsky, under direct tasking from the FSB's Fifth Service. The Czech government imposed national sanctions on the operation the same day. The story then escalated rapidly. Investigative journalists at Denik N and other outlets established that Members of the European Parliament from Germany, France, Poland, Belgium, Hungary, and the Netherlands had been paid by the operation, in some cases to make speeches favorable to Russian positions and in others simply to be interviewed in ways that lent legitimacy to the platform.

On 17 May 2024, the European Union imposed sanctions on Voice of Europe and froze its assets. The sanctions designation document, accessible through the Official Journal of the European Union, names Medvedchuk and Marchevsky as the responsible individuals and identifies the operation as part of a Russian influence campaign aimed at the 2024 European Parliament elections. To my knowledge it remains the only EU sanctions designation against a media operation founded inside the Union itself.

What I want to underline about Voice of Europe is the chain of facts. A Dutch national founds an outlet in the Netherlands. The outlet lapses. A Russian financier acquires control, operating through a Czech address. Members of the European Parliament from six member states accept payments. The combined operation runs for a year before being uncovered. None of this required intrusions into anyone's network. None of it lived inside Microsoft 365. It used the institutions of European democracy as the operational medium, and it did so successfully enough that the EU's response was to sanction itself — in a manner of speaking — by sanctioning an entity that several of its own institutions had unwittingly engaged with.

Smit and the threat picture

The AIVD's annual report for 2025, published on 23 April 2026, opens with a foreword from Director-General Simone Smit that I want to quote at length, because the language is unusually direct for a public intelligence document. The relevant passage reads: "In de tachtig jaar dat de AIVD bestaat, is er niet eerder een dreigingsbeeld geweest zoals het huidige." — "In the eighty years the AIVD has existed, there has not previously been a threat picture like the current one."

The AIVD's institutional predecessors go back to 1945, which gives the eighty-year framing both literal and rhetorical weight. The Director-General isn't asserting that the present is uniquely dangerous in some abstract sense; she's asserting that the documented threat picture, as her service sees it, exceeds the documented threat pictures of all previous moments in the service's history. That includes the height of the Cold War. It includes the period after 9/11. It includes the Crimea annexation in 2014 and the Skripal poisoning in 2018. The claim is severe and it's on the record.

The MIVD annual report, published two days earlier on 21 April 2026, is consistent in tone but more specific in operational detail. It identifies Russian sabotage operations against Dutch public facilities — the AIVD's and MIVD's joint 2026 assessment names a public fountain installation as one of the targeted sites — and notes Russian reconnaissance against Dutch military installations, port facilities, and energy infrastructure. The detail about the fountain is unusually concrete, and it's included in the public report specifically to make the point that critical infrastructure is being defined more broadly than the public would have assumed. A fountain isn't a power station; the reconnaissance against it tells you something about how the adversary thinks about gradient targets.

II. The Chinese Vector

Salt Typhoon: anatomy of a strategic intrusion

In the autumn of 2024, the United States government began to disclose what would become known as the Salt Typhoon intrusion. The basic facts are well established. Beginning at the latest in 2019 and continuing into 2026, a Chinese state-sponsored cyber actor compromised at least nine major United States telecommunications operators — Verizon, AT&T, T-Mobile, Charter Communications, Lumen, Consolidated Communications, Windstream, and at least two additional carriers whose identity remained protected at the time of the public disclosures — and used that access to position itself inside the infrastructure of the American communications backbone.

Senator Mark Warner, who chairs the Senate Intelligence Committee, called it the worst telecom hack in US history. The phrase has been quoted often enough that it now risks losing its force, so it's worth pausing on what it actually means. American telecommunications infrastructure carries the bulk of global Internet traffic that traverses American territory — which is a substantial fraction of all global Internet traffic — and substantial portions of European traffic as well, given how the global routing topology actually works. Sustained access to that infrastructure provides not just the contents of communications, but the metadata of communications, the routing patterns, and the operational topology of the networks themselves. It's a strategic intelligence position of a kind that has no good precedent in the public record.

The exploitation pattern is by now also well documented. The initial vectors were CVE-2023-20198 and CVE-2023-20273, paired vulnerabilities in the Cisco IOS XE web management interface that allowed unauthenticated remote attackers to escalate privileges and achieve root access on affected devices. Both vulnerabilities were disclosed by Cisco in October 2023; by the time they were disclosed, exploitation in the wild was already widespread. Cisco issued patches; the patches were applied unevenly; the actor continued to find unpatched devices, and to use the access it had already established on patched devices for lateral movement and persistence.

On 27 August 2025, the cyber agencies of thirteen countries issued a joint advisory naming Salt Typhoon as a confirmed Chinese state-sponsored campaign and providing extensive technical detail on the actor's methods. The thirteen countries were the United States, the United Kingdom, Australia, Canada, New Zealand, the Netherlands, Germany, Finland, Italy, the Czech Republic, Japan, Spain, and Poland. The advisory identified three Chinese commercial entities — *Sichuan Juxinhe Network Technology*, *Beijing Huanyu Tianqiong Information Technology*, and *Sichuan Zhixin Ruijie Network Technology*[1] — as front companies acting on behalf of the People's Republic of China's Ministry of State Security (MSS). It described over two hundred organizations breached across more than eighty countries.

That number deserves to sit on the page for a moment. Two hundred organizations across more than eighty countries. By way of comparison: the much-discussed SolarWinds intrusion, which was the largest known cyber espionage operation when it was disclosed in late 2020, was assessed to have affected approximately one hundred organizations of intelligence interest, mostly within the United States. Salt Typhoon is at least twice that scale and global in scope.

Three commercial entities and the MSS attribution

The naming of the three commercial entities is doctrinally significant. The Chinese state's approach to cyber operations has long blended military, intelligence, and ostensibly commercial actors in ways that complicate Western attribution methodologies. The People's Liberation Army Strategic Support Force, the Ministry of State Security, and the Ministry of Public Security all conduct cyber operations, and they do so through a shifting constellation of front companies, university research groups, and outright criminal partners. The 2025 joint advisory is unusual in that it names specific commercial entities and ties them directly to the MSS — the Chinese civilian intelligence service — rather than to the PLA.

The MSS attribution matters because the MSS is responsible for strategic intelligence and influence operations against foreign governments. A PLA campaign would suggest a war-preparation framing; an MSS campaign

[1] Note: You may have already guessed it, but I will ***not*** attempt to pronounce those names on stage.

suggests a strategic intelligence collection framing. Salt Typhoon, in other words, is being conducted by the part of the Chinese state apparatus that thinks in decades, not years, and whose work is meant to inform political and economic decisions rather than military ones. The presence of an MSS campaign at this scale tells you something about Chinese strategic patience: they've been inside Verizon since at least 2019, possibly longer, and they haven't used that access for any visible operational effect. They're listening.

Dutch and Italian exposure

The Dutch elements of the Salt Typhoon picture are public but understated. The 2025 joint advisory confirms Dutch participation, which means Dutch intelligence services have observed the actor in Dutch infrastructure. The MIVD's 2024 annual report — the report covering 2024, published in April 2025 — stated that Chinese state-sponsored actors had compromised smaller Dutch ISPs and hosting providers, and identified TU Delft as a confirmed target. The MIVD's 2025 annual report repeats and updates the assessment.

In April 2026, Italian press reported that Sistemi Informativi — IBM Italy's subsidiary providing IT services to large Italian corporates and public bodies — had been breached. Attribution was at the time of publication described as tentative, but the technical signatures matched Salt Typhoon, and Italian intelligence services were said to be working with Five Eyes partners on a fuller assessment. As of the date of this writing the formal attribution hasn't been confirmed, and I won't assert it as established fact, but it's consistent with the broader pattern of European telecommunications and IT-services compromise that the 2025 joint advisory was meant to describe.

The MIVD prognosis: "one layer down"

The MIVD's public annual report for 2025, published on 21 April 2026, contains a prognosis for the year ahead. The Chinese cyber campaigns, the report assesses, will continue to focus on routers, firewalls, and VPN solutions — the perimeter devices that most organizations still rely on. This is the assessment that frames the slide I'm proudest of in the deck, and it's worth setting out the reasoning explicitly.

Most European boardrooms and most European IT strategy conversations remain centered on the application layer. The question that gets asked, when sovereignty is discussed, is some variation on 'where does our Microsoft 365 data live, and what laws apply to it?'. That's a real and important question; I'll spend several thousand words on it in the next section. But the Chinese campaign we have most clearly documented — Salt Typhoon — doesn't operate at the application layer. It operates at the infrastructure layer beneath the cloud. Cisco IOS XE is a router operating system. Citrix NetScaler is an edge gateway. Ivanti Connect Secure is a VPN. Fortinet and Palo Alto firewalls are perimeter devices. None of these are Microsoft 365. None of them are visible in the cloud sovereignty debate as it's conducted in Brussels and The Hague. All of them are where the actor is.

This observation isn't original to me — it's the MIVD's assessment, in a public document, three weeks ago — but it doesn't appear to have penetrated the policy conversation in the way one might expect. The slide I'll show is intended to make the point unmissable. The European policy conversation has settled on the layer above where the attacks live. The Chinese vector is the clearest evidence of this, but as I'll argue below, the Russian vector and the American vector both also operate at layers beneath the cloud sovereignty debate. There's a further point worth making about the Chinese campaign, which is that its sheer scale is itself an indicator of strategic posture. SolarWinds was a hundred organizations. Salt Typhoon is more than two hundred. The Russian campaigns against Ukraine, even in wartime, were measured in tens of high-value targets. China is operating on a scale that suggests not a particular target list but a posture of broad sustained access — the cyber equivalent of having a credentialed employee inside every major telecommunications company in the country, indefinitely. The strategic-intelligence yield of that posture is hard to overstate.

In October 2025, Darktrace published an account of a Salt Typhoon intrusion at a European telecommunications operator, via a Citrix NetScaler edge gateway. The intrusion vector was a known vulnerability; the actor's lateral movement, once inside, was textbook Salt Typhoon technique. The Darktrace report is one of the relatively few public technical accounts of how Salt Typhoon actually behaves once it has entered a network, and it's consistent with the joint advisory in essentially every respect. If you want operational detail, that's where to start.

Volt Typhoon: the parallel campaign

If Salt Typhoon is the intelligence-collection campaign, Volt Typhoon is the war-preparation campaign. The two designations are sometimes confused in popular reporting, but the United States agencies that named them have been careful to distinguish them. Volt Typhoon is the People's Liberation Army Strategic Support Force's positioning campaign against United States critical infrastructure — water utilities, electricity grid operators, transportation systems, and ports. It uses similar techniques to Salt Typhoon at the perimeter — living-off-the-land binaries, abuse of native tooling, exploitation of edge devices — but its targeting is different. Salt Typhoon is inside the telecoms backbone, listening. Volt Typhoon is inside the operational technology of critical infrastructure, positioned.

The 7 February 2024 joint advisory from CISA, the NSA, the FBI, and partner agencies stated the assessment with unusual directness: Volt Typhoon's purpose, the agencies wrote, was to "position themselves on IT networks to enable lateral movement to OT assets to disrupt functions in the event of a major crisis or conflict with the United States." The word 'disrupt' is doing the load-bearing work in that sentence. The intent assessed by the agencies isn't espionage; it's pre-positioning for disruptive action.

Volt Typhoon matters to the European discussion for two reasons. First, the same actor or actors with the same TTPs almost certainly maintain analogous positioning inside European critical infrastructure. The MIVD's 2025 annual report doesn't name Volt Typhoon explicitly in its discussion of Chinese intentions toward Dutch critical infrastructure, but the analytical structure of the report — sustained access to operational technology, focus on energy and water and ports, blending of intelligence and disruptive capability — is consistent with the Volt Typhoon pattern. Second, Volt Typhoon underlines that the Chinese campaign shouldn't be read as primarily commercial intellectual-property theft, which was the dominant Western framing in the 2010s. The campaign's commercial-IP dimension still exists, but the strategic-intelligence and war-preparation dimensions are now ahead of it in priority.

What the 250%/300% numbers tell us

It's worth pausing on the question of historical baselines. In February 2023, Mandiant's Fog of War report provided the first systematic public quantification of how Russian cyber operations had escalated in the year following the invasion of Ukraine. Russian phishing campaigns against Ukrainian targets were measured at approximately 250% of their 2020 baseline; against NATO member targets, at approximately 300%. The numbers are now three years old and have been overtaken by events, but the methodological point still stands: Russian cyber operations against Europe scale with the broader political conflict, and the appropriate baseline isn't last year's operations but the operations of two or three years ago.

The Chinese baseline is harder to establish, because Chinese campaigns are characterized by sustained low-intensity access rather than visible bursts of activity. But the Salt Typhoon disclosures imply a baseline that's been in place since at least 2019, with no obvious diminution since. The appropriate European posture should assume that Chinese strategic-intelligence access to European telecommunications infrastructure is at least at the level documented in the August 2025 joint advisory, and may well be higher, given the lag between intrusion and detection.

III. The American Vector

This is the section that requires the most precision, because it's the section about which European audiences are most uncomfortable, and because the temptation to overreach is largest. I'll try to stay strictly inside the documentary record.

The legal architecture

The legal architecture that gives the United States government extraterritorial reach over data and operations sitting nominally inside European jurisdiction consists of four primary instruments. I'll describe each briefly. The CLOUD Act — the Clarifying Lawful Overseas Use of Data Act — was signed into law in March 2018. It amended the Stored Communications Act to clarify that providers of electronic communication services under United States jurisdiction must disclose data in their custody to United States law enforcement regardless of the physical location of the data. The Act was a direct response to the *Microsoft Ireland* case, in which Microsoft had refused to comply with a United States warrant for data stored in its Dublin datacenter. The CLOUD Act made clear that no such refusal would be available going forward. American providers are obligated to comply.

FISA Section 702, originally enacted in 2008 and reauthorized most recently in April 2024, authorizes the United States Intelligence Community to conduct warrantless surveillance of non-United-States persons reasonably believed to be located outside the United States, for the purpose of acquiring foreign intelligence information. The targets don't have to be suspected of any wrongdoing. The collection is conducted through compelled production from United States communications providers, including the major cloud and hyperscale providers. The Privacy and Civil Liberties Oversight Board's 2023 report provides an unusually clear public account of how the program works in practice; the legal architecture is detailed and the protections for non-United-States persons are limited.

In July 2020, the Court of Justice of the European Union issued the judgment in Schrems II, which struck down the EU-US Privacy Shield framework on the grounds that United States surveillance law — specifically FISA 702 and Executive Order 12333 — didn't provide protections for European data subjects equivalent to those required by EU law. The judgment didn't invent the problem; it made it impossible to ignore. The subsequent EU-US Data Privacy Framework, adopted in 2023, attempts to address the deficiencies identified by the Court, but it remains under legal challenge and most European data protection authorities continue to treat transfers under it as risky.

The fourth instrument is more recent. Beginning in February 2025, the Trump administration began to use Executive Orders — backed by United States Treasury sanctions designations — to apply the legal architecture above as a tool against European institutions whose decisions the administration disagreed with. I'll describe the operational use of this instrument in the next subsection. The point I want to make in this one is that the legal architecture itself wasn't invented in February 2025. It's been there since the late 2000s. What was novel in 2025 was the willingness to use it against European institutions explicitly, with the understanding that European institutions would have no effective recourse.

The Amsterdam Trade Bank precedent

Before turning to the ICC sequence, which is the centerpiece of the American vector, I want to dwell briefly on a Dutch case from April 2022, because it established the operational precedent that the ICC sequence then exploited. Amsterdam Trade Bank was a Dutch-registered bank with Russian ultimate beneficial owners. Following the Russian invasion of Ukraine in February 2022, the United States Treasury added the bank's shareholders to the SDN list — the Specially Designated Nationals list — under the relevant Russia sanctions executive orders. Within days, Microsoft and Amazon Web Services withdrew the bank's access to their cloud platforms. The bank couldn't operate. It filed for bankruptcy within weeks.

What makes the case notable for our purposes is what happened next. The Dutch court-appointed trustees discovered they couldn't access the bank's own administrative records, because those records sat inside Microsoft 365 environments that were no longer accessible. The trustees, who under Dutch law have a fiduciary duty to creditors and a court-issued mandate to do their work, wrote to the Dutch parliament to flag the issue. The Dutch parliament noted the problem. No effective remedy was forthcoming, because the

underlying issue — that a Dutch court order can't compel a United States company to defy a United States sanctions designation — has no available solution in the existing legal architecture.
The Amsterdam Trade Bank case sat in the academic and legal literature for three years as an isolated incident. Some commentators argued it was an artifact of the unusual circumstances around the Russia sanctions; others argued it was a precedent that would generalize. The ICC sequence settled the argument.

The ICC sequence, in detail

On 6 February 2025, President Trump signed Executive Order 14203, titled "Imposing Sanctions on the International Criminal Court." The order sanctioned the ICC's Chief Prosecutor, Karim Khan, by name. Crucially, the order also extended criminal liability under the International Emergency Economic Powers Act (IEEPA) to any person — meaning any natural or legal person, anywhere in the world, subject to United States jurisdiction — who provided Khan or designated court personnel with "financial, material, or technological" support.
The breadth of 'technological' in that formulation is doing very heavy lifting. American technology companies — Microsoft, Google, Amazon, Apple, Meta, and the broader ecosystem of cloud and communications providers — were on notice that continuing to provide services to Khan, after the executive order took effect, would expose them to IEEPA criminal penalties of up to twenty years' imprisonment for the responsible officers. Microsoft's legal counsel evidently advised that the company's exposure was substantial.

On 3 May 2025, Microsoft President Brad Smith traveled to Brussels and announced a five-point European Digital Commitments package. The five points: Microsoft would legally challenge any United States government order requiring suspension of services to a European customer, all the way through United States courts; Microsoft would expand its European datacenter capacity by forty percent by 2027, across sixteen countries; Microsoft would work with European partners on sovereign-cloud arrangements; Microsoft would honor the existing European data residency commitments; and Microsoft would commit to transparency on government access requests.

The pledge was delivered at the highest level and was, I believe, made in good faith. But its existence is itself a significant fact. A company that didn't need to make such a pledge wouldn't have made one. The pledge was a public acknowledgment, by the largest enterprise software company in the world, that the existing situation contained a structural risk that European customers shouldn't have been expected to bear without explicit reassurance. The reassurance was given. Whether the reassurance is operationally adequate is a different question, to which I'll return.

On 15 May 2025, the Associated Press reported — twelve days after Brad Smith's Brussels announcement — that Karim Khan's Microsoft Outlook email account had been disabled. The ICC subsequently announced that it was migrating its operational email infrastructure to Proton Mail, the Swiss end-to-end-encrypted email provider, on an emergency basis. In the longer term, the Court announced its intention to migrate to OpenDesk, the German federal government's open-source workplace platform.

The pledge of 3 May 2025 didn't prevent the account suspension of 15 May 2025. That's the operational fact. The pledge promised legal challenge; the legal challenge, whatever its eventual outcome, didn't arrest the immediate withdrawal of service. The ICC migrated because it had to operate, and the platform it had been using had become unreliable for the workloads it most needed to protect. The institutional decision to migrate is itself a public statement: the Court has assessed that further reliance on the platform is incompatible with its operational mandate.

The sanctions broadened through the summer and autumn of 2025. Four ICC judges were sanctioned in June 2025. Two deputy prosecutors and two further judges in August. Two more judges in December. By the end of 2025, the United States had imposed Treasury sanctions on eight named individuals at the Court, plus the institution itself. The Court's ability to function in its administrative capacities became progressively more compromised; the operational answer, repeatedly, was migration off United States-provided platforms.

On 4 February 2026, Microsoft's Chief Legal Officer Brad Smith testified before the House of Commons Business and Trade Committee in the United Kingdom. Asked directly whether Microsoft could guarantee that data held in its European datacenters wouldn't be compelled by United States authorities under CLOUD Act or FISA 702 procedures, he answered, on the record, that the company couldn't provide such a guarantee. The

same admission had been made some months earlier to the French Senate. These admissions are the most authoritative possible statement of the limits of European sovereignty over American-provided cloud services. They come from the company most invested in being able to give the contrary answer.

Concurrent signals

The ICC sequence is the centerpiece, but it isn't the only signal worth noting. Across early 2025, the new United States administration took a series of decisions that, taken together, indicate a substantial shift in the American posture on cyber defense and trans-Atlantic cyber cooperation. I want to walk through each in some detail, because the cumulative weight of the signals is greater than any single one of them.

On 28 February 2025, Secretary of Defense Pete Hegseth reportedly paused United States Cyber Command's offensive operations against Russia. The pause was first reported by The Washington Post on the basis of unattributed sources within the Defense Department; it was confirmed in subsequent congressional testimony when members of the Senate Armed Services Committee asked the Secretary directly. The operational rationale offered was diplomatic — the Administration was at that time pursuing ceasefire discussions with the Russian government over Ukraine and considered offensive cyber operations to be inconsistent with the diplomatic posture. The substantive consequence, regardless of rationale, was that the United States stopped conducting the operations that had previously been the principal contribution to allied cyber defense in the European theater.

In January 2025, the Cyber Safety Review Board was disbanded. The CSRB had been established in 2022 by the Biden administration's Executive Order 14028 as the federal government's primary mechanism for conducting post-incident reviews of significant cyber events and producing public lessons-learned reports. Its 2024 report on the Microsoft Exchange Online intrusion of mid-2023 — in which a Chinese state actor had compromised the email accounts of senior United States officials including the Secretary of Commerce — was a remarkably candid public document, holding Microsoft's security posture and cloud architecture to substantial criticism. The disbanding of the CSRB in early 2025 was presented as part of broader administrative reorganization, but its operational effect was to remove the federal government's capacity to produce that kind of public assessment going forward.

In December 2025, the Treasury Department withdrew the sanctions that had been imposed in late 2024 on individuals named as responsible for the Salt Typhoon campaign. The sanctions had been part of the formal United States response to the worst telecom hack in our nation's history; their quiet removal a year later wasn't accompanied by any public explanation. The technical attribution of Salt Typhoon to Chinese state actors remains intact — the 13-country joint advisory of August 2025 is unaffected — but the United States response no longer includes the financial-sanctions instrument.

On 24 March 2025, the Atlantic published its account of the SignalGate incident, in which Jeffrey Goldberg, the magazine's editor-in-chief, had been inadvertently added to a Signal group chat in which Vice President Vance, Defense Secretary Hegseth, National Security Advisor Waltz, and other senior administration officials had conducted live planning for the United States military strikes on Houthi targets in Yemen. The chat included the timing of the strikes, the specific weapons systems to be used, and the operational sequence — information that, had it been disclosed to an adversary rather than to a journalist, would have endangered American service personnel. The administration's response was largely to deny that the information had been classified; the more troubling underlying fact — that senior cabinet officials were conducting live military planning on a commercial messaging application not approved for such use — was less remarked upon.
None of these is, on its own, decisive. The pause on offensive operations could be tactical; the disbanding of the CSRB could be reorganization; the Salt Typhoon sanctions withdrawal could be a legal technicality; SignalGate could be an isolated lapse. Taken together, however, they describe a United States in retreat from its previous role in trans-Atlantic cyber defense, and operating with markedly less institutional discipline than was previously the case. The European intelligence services have read them that way, as the Reesink quote makes clear.

The Reesink assessment

On 21 April 2026, Vice-Admiral Peter Reesink, Director of the MIVD, opened the foreword of the service's public annual report with a sentence that has now traveled widely. "Wij bewegen ons steeds verder een wereld van machtsblokken in. Een wereld waarin de Europese Unie door zowel bondgenoot — de Verenigde Staten — als tegenstander Rusland anders bekeken wordt." — "We are moving increasingly into a world of power blocs. A world in which the European Union is regarded differently by both ally — the United States — and adversary Russia."

The phrase 'both ally and adversary', referring to the United States and Russia respectively, is the load-bearing element of the sentence. The Director of a NATO member's military intelligence service doesn't use those words by accident, in a foreword to a public report, with the chain of command and the Minister of Defense having signed off. The sentence is what intelligence officers call a deliberate signal. It signals that the service's working assessment is that the European Union's position vis-à-vis the United States has changed in a way that requires the European Union to factor American action into its planning in a manner that previously would have been reserved for actors in the adversary column.

This isn't a hostile claim. The MIVD doesn't assert that the United States is an adversary. It asserts that the United States now regards the European Union in a way that's different from how it did so previously, and that this difference is operationally significant. The American instruments of compulsion — CLOUD Act, FISA 702, executive orders — are still available, and the demonstrated willingness to use them against European institutions has changed the risk calculation that European planners have to perform. That's a measured assessment, delivered in measured language, and it's on the public record.

IV. The European Response

The SEAL framework

The European response began to crystallize in late 2024 and accelerated through 2025. The most consequential single document is the EU Cloud Sovereignty Framework, version 1.2.1, published by the European Commission's DG CNECT in October 2025. The framework consists of eight Sovereignty Objectives — SOV-1 through SOV-8 — covering legal, geographic, operational, technical, and supply-chain dimensions of sovereignty, and five levels of compliance, SEAL-0 through SEAL-4, designated by the Sovereignty European Assurance Levels acronym.

SEAL-0 is, in effect, no sovereignty: a deployment in which the workload, the data, and the operational control all sit with a non-European provider under non-European law. SEAL-1 is jurisdictional sovereignty: the legal form of the provider is European, but operational control may still rest elsewhere. SEAL-2 adds data sovereignty: the data physically resides within the EU and is processed by personnel and systems subject to EU law. SEAL-3 adds digital resilience: the deployment is operationally independent of non-European supply chains for its core functions. SEAL-4 is full digital sovereignty: all of the above, plus an end-to-end European supply chain including the underlying hardware and the software stack.

It's worth being explicit that SEAL-4 is, in 2026, aspirational. The European semiconductor industry remains dependent on equipment that's itself controlled by United States export law — ASML's extreme ultraviolet lithography machines being the most consequential example, since the relevant export controls also apply to the chips made with them. SEAL-4 may not be reachable in the current decade for many workloads. SEAL-3 is reachable for some workloads, and SEAL-2 is reachable for most. The point of the framework isn't to demand SEAL-4 everywhere; it's to make procurement decisions legible against a stated standard.

Three layers of control

The Dutch government published its Visie op digitale autonomie en soevereiniteit on 18 December 2025. The document is signed by Willemijn Aerdts, the State Secretary for Digital Economy and Sovereignty, and lays out what's come to be called the three-layer model of control. The model distinguishes between legal sovereignty (which authority can lawfully compel access to the data), geographic sovereignty (where the data physically resides and is processed), and operational sovereignty (who has administrative access, and who can withdraw or suspend that access).

The three-layer formulation is more useful than the SEAL framework in some respects, because it makes visible where recent American compulsions have actually operated. The Amsterdam Trade Bank case, and the Khan account suspension, weren't primarily about the geographic layer — the data was, in both cases, physically in the EU. They were about the legal layer (the United States asserted jurisdiction over the provider) and the operational layer (the provider could withdraw service even if the data physically remained). A purely geographic conception of sovereignty wouldn't have flagged the risk; the three-layer model does.

Aerdts's formulation — "soevereiniteit is de vrijheid om keuzes te maken," sovereignty is the freedom to make choices — is, in my opinion, the most precise public articulation of the concept I've seen from a European policymaker. It avoids the absolutist trap (sovereignty as the absence of all dependency, which is unachievable) and the dismissive trap (sovereignty as a romantic abstraction, which is unhelpful). The freedom-to-choose framing makes sovereignty operationally meaningful: at each procurement decision, at each architectural choice, do we have the practical ability to choose otherwise? If we don't, we have a dependency we may not have priced.

The April 2026 tender: framework meets market

On 17 April 2026, the European Commission awarded the first major tranche of its sovereign-cloud procurement — a one-hundred-and-eighty-million-euro framework agreement, the first of its kind — to four European cloud providers under the SEAL framework. STACKIT (Germany), Scaleway (France), and Post Telecom (Luxembourg, in partnership with CleverCloud and OVHcloud) were assessed at SEAL-3. Proximus (Belgium, in partnership with S3NS, Clarence, and Mistral) was assessed at SEAL-2. The award is consequential in three respects.

First, it constitutes market evidence that European alternatives at SEAL-2 and SEAL-3 actually exist. Until April 2026, this was contested in industry; some analysts argued that no European provider could realistically meet the framework's requirements without falling back on American or Chinese infrastructure components. The award demonstrates otherwise. The providers named have undergone the assessment and have been judged compliant. The framework is no longer theoretical.

Second, it sets a precedent for future European procurement at every level — Commission, national, sub-national. Once a framework has been applied successfully once, the political cost of not applying it again rises sharply. National procurement bodies that previously could plead that no compliant providers existed can no longer do so.

Third, it changes the competitive landscape for the hyperscalers. Microsoft, Amazon, and Google are now competing against named European alternatives at named SEAL levels, in a procurement context where SEAL-3 is being treated as the relevant benchmark for risk-sensitive workloads. The five-point pledge that Brad Smith made in Brussels was, among other things, an attempt to position Microsoft as a credible SEAL-2-or-3 provider through its EU Data Boundary architecture. The hyperscalers will continue to compete; the framework now sets the terms on which they compete.

Migrations in practice

Alongside the procurement evidence, there's now a substantial and growing body of operational migrations. I want to name several of them, because the names carry weight.

The International Criminal Court has migrated, as already described, from Microsoft to Proton Mail to OpenDesk. The case is in some ways the most consequential, because the Court is a multilateral institution operating under international law and its migration is itself a precedent for other international bodies. Denmark announced in late 2025 that the entire central government will migrate from Microsoft Office to LibreOffice. The Danish Digitization Agency's public materials describe the migration as a multi-year program with a target completion date in 2028; the announcement itself is signed by the Minister.

The German federal state of Schleswig-Holstein has been migrating approximately thirty thousand civil-service personal computers from Windows to Linux and from Microsoft Office to LibreOffice, since April 2024. The program has had setbacks and the timetable has slipped, but the strategic decision is intact and the migration continues.

The city of Lyon completed in mid-2025 a migration to an open-source workplace suite across its municipal administration. The case is smaller in scale than Schleswig-Holstein's, but operationally relevant because it covers a full municipal administration end-to-end, including the front-line workloads that critics have argued can't realistically be migrated.

The Chief of the Swiss Army, Lieutenant General Thomas Süssli, stated on the record in September 2025 that the Swiss armed forces required an exit strategy from Microsoft cloud services. The Swiss case isn't formally inside the EU framework, but the operational logic is the same.

Airbus has issued a sovereign-cloud tender to replace its existing Microsoft estate, with the stated intention of reaching SEAL-3 across European operations. The tender is in process at the time of this writing; the strategic decision is public.

These migrations matter operationally and they matter as signals. The institutions making them aren't fringe actors. They're major European governments, a multilateral court, and a flagship industrial company. The direction of travel is now legible. The question for any planner isn't whether the migration trend is real, but whether their own institution's position is reasonable in light of it.

The Nixon Shock framing

At the World Economic Forum in Davos in January 2026, Ursula von der Leyen described the present moment as Europe's Nixon Shock. The reference is to August 1971, when President Richard Nixon abruptly took the United States off the gold standard, ending the Bretton Woods system of fixed exchange rates and forcing the rest of the world to rebuild its international monetary architecture in real time. The analogy is, I think, well chosen, and it's worth being clear about what it asserts and what it doesn't.

It doesn't assert that the United States has become an enemy of Europe. Nixon's decision in 1971 wasn't aimed at Europe; it was aimed at addressing a United States balance-of-payments problem. The consequence for Europe was that the previous architecture of dollar convertibility stopped working, and Europe had to construct alternatives. The European Monetary System was built in the 1970s; the euro was the eventual long-term answer. None of this was anti-American; all of it was a response to a structural change that the United States had made for its own reasons.

The 2026 analogy is similar. The legal architecture that underpinned trans-Atlantic digital trust hasn't been formally abolished by the United States; it has simply stopped working as it had been assumed to work. The European response is to build alternatives. The SEAL framework, the April 2026 tender, the migrations of the ICC and Denmark and Schleswig-Holstein and Lyon and Airbus are the digital equivalent of the European Monetary System in the 1970s — institutional architecture being constructed under time pressure, with mixed quality, but with the underlying logic clearly in view.

V. The Observation

I want to close with the observation I'll end the talk on, because it's the observation that has organized my thinking for the past two years.

The European policy conversation on digital sovereignty — the conversation in Brussels and The Hague and Berlin, the conversation that produced the SEAL framework and the April tender and the three-layer model — has settled, almost entirely, on the upper three layers of the digital stack. Applications and office automation: Microsoft 365, Google Workspace, OpenDesk. Cloud platforms and managed services: Azure, AWS, Google Cloud Platform, Scaleway, OVHcloud, STACKIT. Cloud infrastructure and data boundary: the geographic and legal architecture of where the data sits, who has the keys, and which jurisdiction's law applies. This is what SEAL is about. This is what the EU Data Boundary is about. This is what the cloud-sovereignty argument lives inside.

It's a real and important conversation. I support it. I'm not arguing it should be abandoned or de-prioritized. But it's not where the attacks are. The attacks live one layer down — and in many cases, several layers down. Routing, DNS, internet exchanges — the BGP and AMS-IX and NL-ix and SIDN layer. Routers, firewalls, VPN gateways — the Cisco IOS XE and Citrix NetScaler and Ivanti and Fortinet layer. Transit providers, ISPs, hosting — the smaller Dutch ISPs the MIVD has named, the European telcos Darktrace has reported on. Submarine cables, satellites, fiber — the Baltic cables, the transatlantic backbone, the corridors of physical infrastructure that everything else rests on.

Salt Typhoon lives in the routers and the perimeter devices. Eagle S, Newnew Polar Bear, Yi Peng 3 live at the cables. Volt Typhoon — the parallel Chinese campaign against United States and almost certainly European critical infrastructure, discussed in section II — lives at the operational technology and the embedded network layer. The Russian intelligence operations live across all of these, but particularly at the routing and the operational-technology layer. None of this lives in Microsoft 365. The European policy conversation has settled, mostly, on the layer above where the actual contest is taking place.

This is the observation I want to leave with the SCION Day audience. It is, of course, the audience for which the observation is most legible — SCION is itself an architecture at the routing layer, designed to provide path control and resilience at exactly the level the cloud-sovereignty debate is missing. The audience doesn't need to be persuaded that the infrastructure layer matters; the audience is already there. But the audience does, I think, need to take the observation seriously enough to carry it into the rooms where the rest of the European policy conversation is happening.

A working definition of digital sovereignty, for the conditions of 2026: digital sovereignty isn't the absence of dependency but the presence of choice — at every layer of the stack, with realistic exit paths for the workloads where risk acceptance must be low, and with explicit attention to the infrastructure layer beneath the cloud. The conversation in Brussels and The Hague and Berlin needs to move down the stack. That's where the cable was cut. That's where the routers were compromised. That's where the work of the next decade is.

VI. What This Means for Practitioners

I want to close the substantive part of this piece with a short section on what the foregoing implies for the people who actually have to make decisions — procurement officers, infrastructure operators, CISOs of medium-and-large European organizations, and the policymakers who set the framework conditions for those decisions. The piece up to this point has been descriptive. This section is more prescriptive, and the prescriptions are my own. Readers should treat them as one practitioner's reading of the evidence rather than as established consensus.

Risk acceptance is a layer-by-layer decision

The single most important conceptual move that the SEAL framework and the three-layer model invite is to stop talking about 'sovereignty' as a single binary property and to start talking about it as a stack of independent decisions. Each workload sits at some specific level of the stack, and each level has its own legal, geographic, and operational sovereignty profile. The right question isn't 'are we sovereign?' — a question that has no useful answer — but 'at which layers of the stack is our risk acceptance defensible, and at which layers do we need to reduce dependency?'

The answer will, for most organizations, be different at different layers. Email and office productivity for general workforce use may legitimately remain on a hyperscaler with EU Data Boundary protections. Court records, judicial deliberations, and intelligence-sensitive workloads probably shouldn't. Customer relationship management on routine commercial accounts may be fine on Salesforce; the same CRM holding politically sensitive contacts (defense contractors, sanctioned entities' European subsidiaries, court personnel) requires a different assessment. The framework doesn't tell you what the right answer is for your organization; it gives you a vocabulary in which to articulate the answer you've chosen.

Infrastructure layer attention

If the observation that the attacks live one layer down is taken seriously, the operational implications for European organizations are substantial. Most European medium-and-large organizations have invested heavily in cloud-layer security over the past decade. They have less mature programs at the layer of routers, firewalls, VPN concentrators, and edge devices. The Salt Typhoon technique exploits exactly this asymmetry.

Concrete implications include: a serious patch cadence for edge devices, with vulnerability management organized around the perimeter rather than the data center; meaningful network segmentation between the perimeter, the operational technology, and the cloud-fronted workloads; logging and detection at the infrastructure layer of a kind that most organizations currently lack; and the assumption, in any threat model, that the perimeter device itself may already be compromised. The third item — logging and detection at the infrastructure layer — is in my experience the most frequently neglected. Most SIEM deployments are configured to ingest application-layer events. The Salt Typhoon technique would be invisible to most of them, because the actor is operating at the network layer, where the SIEM isn't looking.

For organizations that operate parts of the European Internet backbone — the AMS-IX and NL-ix internet exchanges, the SURF research network, the major Dutch transit providers, the submarine cable operators — the operational implications are larger still. The infrastructure-layer attention I'm describing for medium-and-large organizations is, for these operators, the core of their public mandate. SCION, BGP path validation, RPKI, and adjacent routing-security initiatives are the technical answers; the policy environment in which those technical answers can be implemented is the work of the next decade.

Exit paths, not exits

A theme I want to underline, because it's frequently misread, is that having an exit path isn't the same as exiting. The April 2026 EC tender doesn't mean the European Commission is migrating off Microsoft 365 tomorrow; it means an alternative now exists at SEAL-3 should it become necessary to move. The ICC migration to OpenDesk happened because the Court had no choice; the existence of an exit path for the rest of Europe is what makes the next choice less constrained.

The strategic posture I'm arguing for is one in which European organizations maintain operational continuity with United States providers where that continuity is operationally beneficial, while simultaneously ensuring that the exit path to European alternatives exists, is tested, and could be activated within a defined recovery

time objective if the conditions required it. This isn't a hostile posture toward the United States. It's the posture any prudent purchaser maintains with respect to any supplier whose continued availability is structurally uncertain. The fact that this needs to be argued at all is itself an artifact of how unusual the period from approximately 1995 through approximately 2020 turned out to be — a period in which the assumption of indefinite American supply continuity was treated as a free good rather than as a risk-bearing position. We're now back to the more normal historical situation in which supplier reliability is a variable to be managed.

The Dutch position

The Dutch position deserves a final word. The Netherlands sits in an unusual combination of vulnerability and capability. We are a target of all three campaigns I've described — the Russian sabotage and espionage and influence campaigns are documented against Dutch infrastructure; the Chinese campaign has compromised Dutch ISPs and confirmed Dutch academic targets; the American legal architecture sits underneath every major Dutch institution that uses cloud services. The combination is hard.

But we're also, by international standards, unusually well placed to respond. Our intelligence services have chosen, with the AIVD and MIVD jaarverslagen of 2025, to put more on the public record than any of our peers. Our domestic infrastructure operators — AMS-IX, NL-ix, SURF, SIDN — are world-class in their respective domains. Our political class has, in the December 2025 Visie and the 2026 coalition agreement, articulated digitale autonomie as a leading principle of national policy in a way few of our peers have managed. The framework conditions for a substantive response exist; the question is whether the procurement decisions, the operational migrations, and the infrastructure-layer investments will follow on the timescale the threat picture requires.

That's the question the SCION Day audience is in some respects best placed to answer. The infrastructure-layer expertise sits in this room. The decisions are not, mostly, in this room — they sit in the Ministries and the procurement offices and the boardrooms of the major Dutch institutions — but the technical credibility that informs those decisions is here. My closing argument, on stage and in this piece, is that the technical credibility needs to be more aggressively deployed than it has been to date. The policy conversation will move down the stack only if the people who understand the bottom of the stack make sure it does.

Don Eijndhoven — Founder & Chairman, Dutch Cyber Warfare Community; CEO, Argent Consulting B.V. *Written as background reading for the keynote at SCION Day 2026 Benelux Edition, Amsterdam Science Park, 19 May 2026.*