Seminar Report

Learning from Finland and Estonia: Insights into Digital Innovation, Resilience, and Practical Lessons for Switzerland

Helsinki and Tallinn, 29 August to 3 September 2026

Version 1.0, 7 September 2026

Table of Contents

1 Executive Summary

Finland and Estonia offer two complementary models of national resilience: Finland demonstrates how energy policy, strategic technology investment and institutional trust reinforce long-term sovereignty, while Estonia shows how legal clarity, interoperable digital infrastructure and a whole-of-society cyber doctrine can make a small state highly adaptive. A Swiss delegation of around thirty participants spent six days in Helsinki and Tallinn examining which elements can be transferred to Switzerland - and under what institutional conditions.

The central lesson is that successful digital transformation is not the result of a single platform or technology. It depends on the alignment of law, governance, infrastructure, trust and the ability to cooperate across institutional and national boundaries.

Five findings frame the report:

First, energy is the foundation of digital sovereignty rather than a side condition. Finland generates electricity at roughly forty euros per megawatt hour, against more than double that in Switzerland. That single number explains much of what follows: the data centres, the artificial intelligence workloads, the industrial base. Estonia's Minister of Energy and the Environment put the dependency in one sentence that framed the entire week. *"If there is no power, then of course we are all cyber safe as well."*

Second, Estonia's real export is not a technology but an architecture of three simultaneous layers, legal, organisational and technical. A digital signature was made legally equivalent to a handwritten one in December 2000. Authoritative registers each have a named accountable owner and are bound by a once-only principle. Only then comes the technical data exchange. Copy one layer and you get nothing. As Raul Kaidro, CEO of RaulWalter, told the delegation: *"If you take the copy of X-Road, you get a portal. If you pass the digital signature law, you get a legal instrument that nobody uses. The value is in the combination, and the combination for us took a decade."*

Third, trust is maintained rather than achieved. Finland is the first country in the world to bring a deep geological repository for spent nuclear fuel to the point of licensing. That outcome was produced not by engineering but by thirty years of transparency, to the point where the final two candidate municipalities competed to host the facility. Estonia's Information System Authority fined its own parent ministry for inadequate IT security, expected budget retaliation, and received a budget increase instead.

Fourth, the economics of cyber defence have turned in favour of the attacker, and Estonia's answer is doctrinal rather than technical. Lower the cost of defence, raise the cost of attack, and deny the political payoff. The third of these is the least obvious and the most instructive. Estonia deliberately normalises the reporting of

incidents, so that silence rather than disclosure becomes the thing that worries the public.

Fifth, and most uncomfortably, Estonia could not build its own system today. Not for technical reasons, but because the information environment has changed. The delegation was told this plainly at the Information System Authority. For Switzerland, currently debating its own electronic identity, that is not an academic observation. It is a statement about closing window.

The report closes with eight concrete recommendations, ranging from the design of the Swiss e-ID to an immediately actionable proposal for Swiss participation in the NATO exercise Locked Shields.

2 Detailed Report

2.1 Seminar Leadership, Delegation and the Question

The seminar took place from 29 August to 3 September 2026, beginning in Helsinki and continuing in Tallinn. The delegation and the seminar were jointly led by Dr. Elisabetta Depace, Public Affairs and International Activitiesand and Andreas W. Kaelin, co-founder, Member of the Board and CEO of Alliance Digital Security Switzerland ADSS. Their joint leadership covered the substantive direction of the programme, the guidance of the delegation and the connection between the discussions across both countries. The programme formed part of ADSS's long-running series of international study seminars and combined policy dialogue, technical briefings and institutional visits.

Dr. Elisabetta Depace formally opened the seminar in Helsinki and again opened the official Tallinn conference. In both cities, she gave the opening remarks first and then handed the floor to National Councillor Franz Grüter, President of ADSS, and Andreas W. Kaelin. This sequence reflected the shared leadership of the seminar: Dr. Depace and Kaelin guided the delegation and programme jointly, while Grüter framed the discussions from the perspective of ADSS and Swiss public policy. In Helsinki, the opening was followed by the welcome from the Swiss Embassy in Finland; in Tallinn, the opening remarks were followed by an address from Estonia's Minister of Energy and the Environment, Andres Sutt, before the contribution of Raul Kaidro, CEO of RaulWalter.

The group brought together representatives from politics and the federal administration, academia, the armed forces and cyber-security community, global technology companies, Swiss industrial and family-owned businesses, and organisations working on critical infrastructure, testing and international cyber cooperation. This mix of public-sector, private-sector and technical perspectives was central to the seminar's whole-of-society approach.

The framing question was posed most sharply not by the delegation but by its hosts. At the e-Estonia Briefing Centre, the delegation was reminded that Estonia rebuilt its state from nothing after 1991 with 1.3 million inhabitants and no natural resources beyond some oil shale. The adviser then turned the comparison around. Switzerland has nine million people, and it has money. *"So, I would say you have no excuse."*

Sophie Steiner Kernen, Deputy Head of Mission at the Swiss Embassy in Finland, welcomed the delegation on behalf of the Swiss Embassy in Finland and noted that 2026 marks exactly one hundred years of bilateral relations, that Switzerland was among the first states to recognise Finnish independence, and that more than 140 Swiss companies operate in Finland today. She also set out the limits of similarity with unusual candour. Finland joined NATO in 2023 and shares a land border with Russia of more than 1,300 kilometres, and on several questions of foreign policy the two countries do not always agree. Her formulation was memorable: "We are very happy to agree that we don't agree."

2.2 Energy Is the Foundation

At the VTT Technical Research Centre in Espoo, Jani Halinen, Vice President for Nuclear Energy, opened with a comparison that recurred throughout the week. The average spot market price of electricity in Finland runs at approximately EUR 40 per megawatt hour. The comparable Swiss figure was more than double.

The explanation lies less in the generation mix than in market integration. Roughly forty per cent of Finnish electricity comes from nuclear and around a quarter from wind, which is not radically different from Switzerland. But Finland forms a single price area within the Nord Pool market and has strong grid connections, whereas Switzerland sits inside the Central European grid. As Halinen put it, Switzerland is paying the price for being part of that grid. The trajectory is equally instructive. Emissions from the Finnish energy sector have fallen roughly eighty-eight per cent from their 2003 peak, coal will be banned from 2029 and is already in practice gone, and the country targets carbon neutrality by 2035. When Olkiluoto 3 came online three years ago, it did not displace other domestic generation. It displaced imports from Sweden, Norway and, until it became impossible, Russia.

What struck the delegation most was not the technology but the political culture around it. Finnish energy policy is explicitly technology neutral. The targets are fixed, the means are not. Nuclear power has enjoyed high public acceptance for one to two decades. In Halinen's words: *"Nuclear is not a political issue; it's more of a pragmatic issue. How do we reach these targets that we have set for our whole power system?"*

VTT itself illustrates a second structural point. It is fully state owned and independent, with an annual operating income of around EUR 300 million and just under 2,500 staff, and it has produced more than sixty spin-off companies whose combined private

equity funding exceeds a billion euros, among them IQM Quantum Computers and Steady Energy. Halinen's summary of the model was direct. If there is no industry, VTT creates the spin-off and creates the industry itself.

On small modular reactors, presented by Kim Stålhandske, the regulatory half is the more transferable one. Finland's new Nuclear Energy Act was approved in the summer of 2026 and enters into force in January 2027, replacing legislation from 1987. Licensing becomes risk graded, which means small reactors do not require the protective structures of large plants and emergency planning zones are set case by case rather than by fixed distances, permitting siting close to populated areas and therefore connection to district heating. Licensing also becomes neutral technology, so safety requirements are no longer tied to solutions, and the decision in principle, the site assessment and the concept assessment become separate processes a developer can advance independently. Steady Energy's LDR50 is a heat-only reactor of 50 megawatts thermal operating at roughly 150 degrees Celsius, against over 300 degrees in electricity-generating reactors, which permit radically simpler safety systems. A full-scale pilot is under construction at Salmisaari, a former coal plant in central Helsinki, with operations planned for spring 2027. Stålhandske was equally candid about what remains unsolved: the supply chain, serial factory production, and an operating model, since small municipal utilities can support neither an emergency organisation nor a waste solution alone.

The presentation that made the strongest impression was delivered by Erika Holt, Lead for Nuclear Back-End, on Finland's deep geological repository for spent nuclear fuel. Disposal takes place at more than four hundred metres depth, with fuel encapsulated in copper canisters and surrounded by bentonite clay. The regulator gave its safety clearance in early August 2026 and the operating licence is regarded as a formality. Operations are designed to run for one hundred years, and the safety case is modelled over one million years, including future ice ages. Posiva, the implementing company, is the structural counterpart to Switzerland's Nagra, with which it cooperates closely.

But the part that belongs in a report on digital resilience is the social one. Finland narrowed thirty candidate sites to seven, then four, then two. And the last two municipalities did not resist. *"They were fighting over who would get the site."* Both were existing nuclear communities whose families had worked in the industry for decades. They understood the economics and they trusted the safety case. Holt was explicit that Finland had not planned to be first. *"Finns are very modest. We didn't plan to be the first in the world. We thought Sweden would be, the United States would be. Even Switzerland was quite ahead in this game some years ago."* What produced the outcome, in her account, was trust and transparency: clear roles between research, supply chain, regulator and government, credible authorities, proper funding, and openness about what is known and what is not. For Switzerland, where high-level waste is expected

underground around 2060 subject to licensing and referenda, the relevant lesson is not geological.

2.3 Sovereignty You Can Buy

At ICEYE in Espoo, Philipp Hermann, Vice President Missions Germany, presented a company that has travelled a distance in eight years that few technology firms travel in thirty. Founded in 2012, ICEYE launched its first satellite in 2018 and now operates 76 satellites in low earth orbit, making it the world's largest commercial operator of synthetic aperture radar satellites. Radar penetrates clouds, darkness, smoke and even volcanic ash. According to NASA figures cited in the presentation, any given point on earth is obscured by clouds roughly two thirds of the time, and optical satellites see nothing there. Resolution reaches sixteen centimetres, and a satellite weighs around 200 kilograms, which the company compares to a small washing machine.

Speed is the business model. ICEYE produces one satellite per week and intends to double that next year. It guarantees twelve months from contract signature to a launched system, and existing satellites are updated over the air. In December 2025, ICEYE and Rheinmetall won a contract with the German Bundeswehr worth approximately EUR 1.7 billion, running to the end of 2030 with extension options. Ukraine is where the capability was hardened. ICEYE has been engaged since summer 2022, and figures published by Ukraine itself record more than 4,000 images by June 2024. Hermann's explanation of the company's performance was blunt. They have had to prove themselves there every single day since.

The concept most relevant to Switzerland is what ICEYE calls federation. Few states can afford a large constellation, and most acquire two to four satellites. Under federation, each nation retains full sovereign control of its own satellites but connects them through a shared software layer under pre-agreed operational rules, so that several small constellations function as one large one. Finland, the Netherlands and Poland are already under contract. A member of the delegation asked the obvious question. Why pursue a multi-billion-euro European programme when the capability can be bought as a service? Hermann's answer, in substance, was that technically it is possible and politically it is not.

Asked what Helsinki offers that Germany does not, Hermann, a German national with a background in the conventional defence industry, answered without hesitation. Legislation, state support, accompaniment by partner universities, and a state that is simultaneously customer and investor. He called it a resilient package thought through from end to end, something he had never encountered as a German citizen. He was equally direct about the security environment. Attempted recruitment of staff by foreign services is a normal reality, and all employees are vetted by the Finnish intelligence service.

IQM Quantum Computers, founded in 2018, has approximately 400 employees drawn from more than fifty nationalities and has raised around USD 600 million. In June and July 2026, it listed publicly on Nasdaq and in Helsinki, the first company in the European quantum sector to do so. Its origin story is the most instructive part for a policy audience. Finland, one of the co-founders said, had been a poor country, and if you want to build something bigger than is possible you have to look for another way. Then came the decisive question. Who can buy a quantum computer? *"We decided it has to be the Finnish government."* Through innovative public procurement, the Finnish state and VTT bought first a five-qubit system, then twenty, then fifty, and are now scaling towards three hundred. When the partnership began, the quantum computer did not yet exist. On the day of the visit, a EUR 650 million EuroHPC investment in a Finnish AI factory was announced across the road at CSC, including an IQM quantum accelerator worth EUR 33 million.

The figures that matter most to a cyber security readership were presented by Jouni Flyktman, Vice President for Defense and Security, who spent twenty years in the Finnish Defence Forces before joining IQM. Quantum computing, he noted, is only one of several quantum technologies that will shift the balance of power, and quantum communication, sensing and navigation may matter as much. The consequences he named include the detection of submerged submarines and the end of dependence on satellite navigation.

Then came the sequence that should concentrate any Swiss reader's attention. The estimated number of physical qubits required to break RSA encryption has fallen by more than two orders of magnitude in six years, from approximately twenty million in 2020 to approximately one million in 2025 and approximately one hundred thousand in 2026. Extrapolated, that curve intersects published hardware roadmaps around 2030, and Google has set an internal target of readiness for post-quantum cryptography by 2029. Flyktman also presented the counterargument, noting that Peter Shor, whose algorithm underlies the threat, has expressed scepticism that it will prove practical at scale. The reality, in his words, is somewhere in between. A member of the delegation raised the sharpest objection of the session. If the world is migrating to quantum-safe algorithms anyway, is the capability being developed one that will only ever decrypt intercepted historical traffic? That is precisely the problem known as harvest now, decrypted later, and it is the reason migration must begin before the threat materialises rather than after.

2.4 Energy, Resilience and the Foundations of the Digital State

At the official Tallinn conference, Mr. Andres Sutt, Estonia's Minister of Energy and the Environment, spoke immediately before Raul Kaidro's contribution. Minister Sutt addressed the important connection between energy and resilience, while also pointing out the importance of cross-border collaboration in tackling shared

challenges and building stronger, future-ready societies. His intervention reinforced one of the seminar's central conclusions: digital sovereignty depends not only on secure digital systems, but also on resilient physical infrastructure and sustained cooperation with trusted partners.

Raul Kaidro, CEO of RaulWalter, then articulated one of the clearest structural lessons of the Tallinn programme. The technology, he argued, was and remains the easy part - and it can be bought. Estonia's digital society works because legal, organisational and technical foundations were developed together as one coherent system.

The legal lawyer came first. Estonia's Digital Signatures Act entered into force in December 2000 and did one thing that mattered. It made a digital signature legally equivalent to a handwritten one. Not comparable, equivalent. The domestic decision moved faster than European law could follow.

The organisational layer is less visible and far more work. Estonia maintains authoritative registers for population, business and property, and each has a named owner accountable for the accuracy of its data. Above them sits the once-only principle, under which the state may not ask a citizen for data it already holds. Kaidro was precise about its nature. It is not a technical feature but an administrative constraint, one that forces institutions to rely on each other's data rather than collect and maintain their own copies.

Only then comes the technical layer, which is X-Road. And then the conclusion that should be quoted in full in any Swiss discussion of digital government:

"If you take the copy of X-Road, you get a portal. If you pass the digital signature law, you will get the legal instrument that nobody uses. The value is in the combination, and the combination for us took a decade."

At the e-Estonia Briefing Centre the technical explanation used a domestic analogy. Valuables are not kept in one safe but distributed, some in the attic, some in the cellar, some in the garden. There has never been a central super-server. Citizens' data is scattered across thousands of databases, each holding its own fragment, and the reasoning was stated without diplomatic softening. There is one particular neighbour that is very interested in all of it, and that neighbour now has to work a great deal harder. *"You have to hack into fifteen databases instead of one. And we will detect you from the first attempt."*

Two design decisions give the architecture its character. Some queries require the data subject's own eID as a split key, so that without a digital signature the connection does not open, which means an employer cannot run a background check without consent. And governance is legislated rather than negotiated: a specific law regulates who may connect to what, with the Information System Authority as the filter. As the briefing centre put it, it is not a list where you tick the boxes of what interests you. You get

what the law allows you to see. Two objections from the delegation deserve recording, because they are the right ones. Such a system demands a very high degree of standardisation, and it is only as good as the data quality of its critical nodes.

Kaidro's description of ordinary business life was more persuasive than any statistic. Contracts and annual reports are digital, one-party signs and forwards, and minutes later everyone holds the same legally binding document. Nobody asks whether a digital signature is acceptable, because it simply is the signature. *"We've actually reached the point where we really don't trust paper."* His formulation of success criterion deserves to be adopted more widely: the success of digital government is not measured by how impressed people are with its technology, but by when they stop noticing it.

Estonia's identity card has been mandatory since 2002, a risky decision mitigated by a compromise. Possession was compulsory, digital use was not, so when the state decided a few years later to make the switch to digital, the tool was already in every pocket. And for five or six years it was thoroughly unpopular. In the words of the briefing centre, people used to say the best use for this piece of plastic was to scrape the ice off the windscreen in winter. The card had arrived before the services, cost more than the document it replaced, and offered only a promise. The turn came through the banks, when it replaced the randomised code cards then used for online banking and became overnight the single access point to every bank account a person held. Redundancy became doctrine only later, and for a concrete reason. In 2017 a vulnerability in the chip affected the entire national card base, and although most cards could be repaired remotely, the rest had to be physically replaced. Estonians today deliberately hold more than one credential, so that if one fails another can be used to suspend it and order a replacement.

Priit Liivak, Chief Government Technology Officer at Nortal, offered the cleanest periodisation. The first era digitised the paper forms, with the administration at the centre. The second redesigned entire systems for digital. The third is personal government, in which the state approaches the citizen. When a child is born, both parents receive a proposal setting out their entitlements and need only supply a bank account and choose which parent receives the benefit. Liivak also addressed federal states directly, and Switzerland by name. The struggle in the United Kingdom, Germany and Switzerland is the same, and Estonia's own answer is not centralisation. Every government entity is responsible for its own data, interoperability and systems, and that decentralisation is what produces resilience under attack. His recommendation for federal countries is that cantons and municipalities retain control and responsibility while the federal level mandates a standard, namely the use of a proven secure exchange platform. Development costs are falling, and nobody has to

solve secure data exchange for themselves, because it is inherited from the national trust backbone.

2.5 Trust Is Maintained, Not Achieved

Every account of Estonian cyber security begins in 2007, and the delegation received the political version rather than the technical one. The trigger was the Bronze Soldier, a Soviet war memorial at the edge of Tallinn's old town. On Russian holidays it became a gathering point, and Estonians who displayed their own flag there were attacked. Prime Minister Andrus Ansip concluded that this was not tolerable in one's own capital, and the monument was relocated to a cemetery. The briefing centre's explanation of the reaction was direct. How do you exert influence over a place you occupy? You put up your statues, and you change the names of the streets.

What followed was the only riot in Estonia's modern history. In parallel, public-sector databases, every media house and the entire financial sector were attacked simultaneously. The response revealed the architecture. Several databases performed emergency shutdowns that locked out even their own administrators, each protecting its own fragment. The country worked on paper for some weeks, but the data held. The internal verdict was delivered with dry humour: *"It is the best test run for our X-Road system."* The emotional dimension was not glossed over. It scared them, as a reminder that they were not safe even sixteen years after regaining independence. Notably, Estonia, then a recent member of both NATO and the European Union, deliberately invoked no NATO article and handled the crisis alone. The institutional consequences are visible today. They include the NATO Cooperative Cyber Defence Centre of Excellence, the EU IT agency, the Locked Shields exercise, a cyber unit within the volunteer Defence League, and, from 2008, blockchain timestamping of every data movement between databases.

The data embassy Estonia has maintained in Luxembourg since 2014, holding backups of its most critical databases, illustrates the same instinct. The innovation was legal rather than technical, because the concept of diplomatic immunity and of the diplomatic pouch was extended to data, and the work required lawyers, engineers and public administration simultaneously. A Swiss participant noted that the International Committee of the Red Cross has moved its data out of Switzerland to a similar arrangement in Luxembourg and expressed frustration that Switzerland had missed the opportunity to offer such a construction itself.

Estonia's data tracker allows any citizen to see every transaction concerning their own data on X-Road. In healthcare, every enquiry is tied to a named individual, because the physician logs in with their own eID. Andreas Lehmann, Director of Lehmann & Partner OÜ and Swiss honorary consul in Estonia, supplied the case that demonstrates the mechanism. In February 2012 a paramedic at a defence medical centre was

hospitalised after a stroke. Doctors and nurses outside his circle of care accessed his file, some after midnight and out of curiosity, and material reached the press. They were all dismissed. It has not happened again. His summary of the underlying principle was that there is no elevated status for civil servants, doctors or law enforcement staff. The citizen also holds a genuine power over their own health record, which can be locked unilaterally. The cost is real and was stated plainly. After a serious accident, the emergency department begins from a blank page and cannot even see a blood type. Most people leave the record open.

At the Estonian Information System Authority, known as RIA, the delegation asked whether the police effectively hold a master key across X-Road. The answer was no. Police may read specified databases, with specified information, for specified purposes, and query patterns that fall outside the norm are flagged, with staff disciplined or dismissed. The qualification, which belongs in the record, is that police and security authorities are excluded from the data tracker, because otherwise they could not do their work, and are subject to a separate oversight mechanism. Substantial investigations require a court order.

The single most transferable governance finding of the week also came from RIA, and it concerns institutional credibility rather than technology. RIA is an authority rather than a centre, and the distinction is that it may supervise and impose fines. It used that mandate against its own parent ministry, which was not performing adequately on IT security. The expectation inside the agency was that the budget would suffer.

"We were thinking, okay, maybe now our budget will get cut. But everything went okay. And given the times, we are one of the few authorities whose budget has been increased. So finding your superiors works."

Supervision under the NIS2 framework has expanded sharply, from roughly 3,000 subjects under the previous cyber security law to close to 6,000 under the current one. Fines are not one-time events. If the problem is not fixed, they return the following month, and each year a different sector is the supervisory focus. RIA also volunteered the necessary caveat, which a Swiss readership should note. Passing the documentation review does not mean an organisation is secure, because it is not a penetration test. The Estonian information security standard itself was adopted from the German BSI standard, translated and progressively adapted, and is ISO 27001 compliant for international purposes. Recognising that a one-person company cannot implement ISO 27001, RIA is building a lighter version for small and medium enterprises and offers grants of up to EUR 60,000 to those that improve their security using its methodology.

Asked how Estonia built public acceptance for a system of this transparency, the RIA representative gave an answer that was not on any slide:

"I think we did it at the right time and built up trust by all the different incidents that we had, being really public and open about them. But now, when you have misinformation and you can lie and make claims about everything, it's much harder to open something like that. For those who want to try it now, I don't know how to do it, to be honest."

Estonia could not build its own system today. Not for technical reasons, but because the information environment has changed. For a country currently debating its own electronic identity, that is the most consequential sentence of the entire seminar.

2.6 The Economics of Cyber Defence

The clearest strategic thinking of the seminar was presented at Nortal by Andres Raieste, Senior Vice President and global head of public sector. Nortal employs roughly 3,000 people and is permitted by the Estonian government to state that it has implemented approximately forty per cent of everything in the Estonian state. His thesis was economic: the economics of cyber defence have turned in favour of the attacker.

Estonia's own history supplies the reference case. In 2007, in what became the world's first national-scale cyber attack, chainsaws were used to cut cables to halt attacks on critical infrastructure. Nobody was prepared. The structural problem was cost asymmetry. If an adversary commits a hundred million euros to cyber operations against the Baltics while the defender has eleven million, the gap is an order of magnitude. Estonia could never fund symmetric defence and therefore had to defend asymmetrically from higher ground and finding that ground became the strategy itself. Twenty years on, his assessment is that the world has arrived where Estonia was. Exploits are now found and used faster than defenders can remediate, with artificial intelligence a substantial part of the reason.

The refined doctrine has three aims. Lower the cost of defence. Raise the cost of attack. And deny the political payoff, which Raieste considers possibly the most important of the three. That third aim is the least intuitive. Russian cyber attacks in Estonia are not conducted against a bank to steal money. They are conducted to make the government look weak, and they typically occur during election periods.

Four policies follow, and each is transferable. **The first is to abandon the perimeter and ask instead what cannot fail.** It is not economic to protect everything equally, so certain base registers that constitute the continuity of the state are protected and made redundant to the point where even physical destruction produces no lasting damage. Raieste was candid that this is the hard part, because if the question is put to a multi-party parliamentary government you do not get a good answer. It requires strong institutions capable of prioritising.

The second is to choose the ground. Rather than fighting along an indefinite perimeter, consolidate the fight onto a small number of hardened common

components, above all identity infrastructure. Most attacks are unsophisticated but massive in scale, and the easiest entry point is authentication. Harden that until attacking it becomes uneconomic. The technical name is digital public infrastructure. The policy name is the national trust backbone, because everything else inherits trust from it, including telecommunications operators, utilities, local government and the wider economy.

The third is to inherit security through standards. The national standard must be considerably stricter than the collective baseline. Where general frameworks still discuss antivirus, the Estonian standard requires, for the highest security tier of government systems, that nothing in a database may be edited or deleted. Records are append only and cryptographically chained. The consequence is economic rather than merely technical. An average developer needs to know less about security, because it is inherited from the standard and the components, and that is what makes the construction of secure systems scalable.

The fourth is to deny the political payoff through radical transparency. This was the most counter-intuitive idea of the week. If the adversary's objective is modification of the media space, the countermeasure is communicative rather than technical, and incidents are deliberately normalised.

"We want to build up conditions in the entire population that something is constantly happening. That it's normal, it's normal that you read in the news that there was some incident. And if there is greater silence, then you worry: is somebody hiding something from me?"

RIA made the same concrete doctrine. Since the invasion of Ukraine, distributed denial of service attacks has become part of the diplomatic toolbox. After parliament declared Russia a terrorist state, there was an attack. After the removal of a Soviet monument, there was an attack. After President Zelensky addressed the Estonian parliament, there was an attack. *"It was like a KPI for us. You know, we did something good."* An attack that confirms the correctness of a country's policy has failed at its actual purpose.

Two further points from the same session deserve recording. Raieste argued that machine-speed defence is a regulatory problem rather than a technical one. His scenario is an attack underway at a hospital, with two minutes to decide whether to take a department's X-ray machine offline. Who makes that decision? Existing regulation was written for attacks at human speed, and courts expect evidence of deliberation, so institutions across Estonia are working on how to formalise such decisions in advance. And Estonia extends the Nordic total defence doctrine into cyber through voluntary corps and cyber reservists. The delegation raised the obvious objection: mobilising cyber experts raises the security of the state while lowering it at

the bank or insurer they come from. The answer was that these are precisely the most valuable people, because banks, telecommunications operators and critical infrastructure must in any case be connected into a shared threat picture. Cyber defence in Estonia is a fully civilian effort, carried substantially by the private sector, and the talent pool is small in a way Switzerland will recognise. Recruiting a national head of cyber security in the United Kingdom yields a thousand applicants. In Estonia, in his phrase, there are two icebergs to choose from.

Raieste also named the crisis that unsettles the model. Europe inherits trust upstream, increasingly from United States cloud providers, and that has become a sovereignty question. France has decided at state level to migrate away from Microsoft Windows and Office across some 2.5 million government devices, framed explicitly in terms of digital sovereignty. His summary of the European predicament was terse. Europe is buying American weapons and American office software. This is a company position and is reported here as such. Estonia's own practice is more nuanced, as the delegation heard at RIA the same afternoon. There is no central government decision on Microsoft; each agency decides according to its own risk profile and budget, and the Ministry of Foreign Affairs is an exception that does not permit it.

On attribution, Raieste was realistic. National-scale attacks do not originate from an offensive unit in a Kremlin basement but run through a supply chain of criminal organisations and freelancers funded by state actors. To invoke Article 4 of the North Atlantic Treaty or Article 51 of the UN Charter, attribution must occur, and that is precisely the value of the NATO Cooperative Cyber Defence Centre of Excellence. RIA described its own practice in the same terms, with assessments of highly likely and likely, built from many small indicators and assembled through exchange with EU and partner services. Russia remains the principal threat and Chinese actors are increasing.

2.7 The Centre of Excellence and Locked Shields

The NATO Cooperative Cyber Defence Centre of Excellence occupies an unusual institutional position. It is NATO accredited but not part of the NATO command structure, and its director reports to no one within NATO. Accreditation principally provides legal status together with a measure of diplomatic immunity, and the practical consequence is intellectual independence, since the Centre can disagree with NATO doctrine in public. Estonia always provides the director and Germany the deputy director. With around seventy staff, it is by a wide margin the largest of NATO's centres of excellence measured by participating nations, and it began in 2008 with eight. Non-NATO contributing participants include Switzerland, Austria, Ireland, the Republic of Korea and Japan, and Ukraine has been an official member since 2022. Switzerland currently seconds two people, including its National Representative, who works in the strategy branch.

The law branch addresses a problem that is easy to underestimate. Neither the Geneva Conventions nor the UN Charter mention cyber or the internet, and the body of international law applicable to armed conflict predates the technology entirely. Is a computer virus a weapon? Within NATO the position has been consistent since the Wales Summit of 2014, where allies first acknowledged that a cyber attack could trigger Article 5. It was reaffirmed at Warsaw in 2016, when cyberspace was declared an operational domain, and again at Brussels in 2021, with deliberate strategic ambiguity as to thresholds. A point of precision worth making in any Swiss discussion is that the Tallinn Manual is an interpretation of international law rather than international law itself.

Locked Shields is the world's largest live-fire cyber defence exercise. The 2026 edition brought together 41 nations and more than 4,000 participants in 16 multinational teams, defending critical infrastructure, air defence and electronic voting systems. Nations are asked explicitly not to compete alone but to partner with at least one other nation. Switzerland exercised together with Germany, Austria and Luxembourg, with the main exercise team located in Kalkar in Germany, and that team placed second overall. The scenario is deliberately fictional, for two reasons. Participants would otherwise dispute whether their own country uses the systems being defended, and everything in the exercise must remain unclassified. The moment a nation writes Russia into an inject, the material becomes classified, and then the work is difficult within a nation and nearly impossible between nations. The artificial scenario is what makes cross-national exercising possible at all.

Economics deserves attention from anyone who has ever budgeted an exercise. Around 600 people are required to organise and run Locked Shields, against a Centre of seventy. The remainder are volunteers, seconded by nations and industry or participating on their own initiative. They receive meals, a workstation, coffee and a closing social event, and they pay for their own flights and accommodation. The Centre has to turn people away because there are more volunteers than it can accommodate. Siemens supplies the power grid hardware for roughly EUR 35,000 per year in maintenance and updates, with no licence cost, where commercially the hardware and software would represent a high six-figure annual value, and provides personnel to operate, evaluate and attack the systems. Asked to estimate the budget, the delegation guessed five million euros. Locked Shields costs a little under one million.

Within the exercise sits a strategic decision-making component aimed at senior national decision makers, using the instruments of national power under cyber crisis conditions. On the second day, nations are asked to bring private sector actors into their national teams, which makes it an explicit whole-of-society approach. The framing was crisp: if nations do not have a specific and clear strategic objective, all winds are favourable.

RIA described a three-tier escalation structure that is among the most directly transferable models the delegation encountered. First, CERT-EE responds. If the incident is protracted, the government IT centres release their experts, whose entire staff is enrolled in the cyber reserve. If that capacity is exhausted, the Cyber Unit of the Estonian Defence League is called upon, consisting of private sector volunteers. Exercises are physical: in a hospital exercise, participants entered the critical care unit and had to identify which machines required replacement. One question raised by the delegation was not resolved and should be recorded honestly. Under international humanitarian law, the use of civilians in military or military-adjacent operations is problematic. RIA's position is that these are not military operations and that the Defence League consists of volunteers rather than armed forces, although the League sits under the Ministry of Defence. For Switzerland, which is likely to consider militia models for cyber, that unresolved question is not academic.

2.8 The Human Layer

For a delegation of security professionals, the most immediately relevant finding of the week concerned neither architecture nor doctrine. Estonia is setting negative records. Citizens and companies now lose approximately EUR 29 million a year to fraud, with a sharp increase between 2023 and 2024. Almost all successful incidents are phishing and fraud in which people surrender their PIN codes. There is no malware and no technical compromise. In the words of the briefing centre, it is simply a matter of tricking people.

The cause of the step change is specific, and it was reported independently by two organisations on two different days. Artificial intelligence learned Estonian. The language is notoriously difficult, and until roughly 2023 machine-generated text made enough mistakes that fraudsters could not credibly impersonate a health authority or a bank. The language was, in effect, an unintentional firewall. Once artificial intelligence solved it, the barrier fell. There is no equivalent protection for German, French or Italian, which have been well modelled for far longer. The Estonian experience is therefore not a warning about something that might happen to Switzerland. It describes a threshold Switzerland crossed earlier and less visibly.

The inclusion mechanism Estonia built for this problem is worth noting for its ordinariness. In the 2000s, public libraries were equipped as internet access points, originally so that any citizen could examine the mayor's salary or the results of public procurement. The lasting effect was different. Libraries became a safe place for older people to ask questions without repeatedly troubling their grandchildren. Librarians are now being trained in artificial intelligence, because that is what elderly patrons are asking about, and because it is the librarian's responsibility to decline when someone tries to hand over their card and PIN.

The most useful single example of the week was presented by Nortal. An e-resident of Estonia who owns a company there has published an open-source solution that files and pays his company's monthly taxes through a commercial AI assistant. The agent queries the tax authority for the amount owed, a QR code appears as the authority's second factor, and on confirmation the tool contacts his bank, prepares the payment and completes it. Mechanisms are the important part. The solution imitates human interaction. It opens the web page, signs in and loads the QR code. There is no interface designed for machines. Nobody authorised it, and the bank had published no such interface at the time. Nortal's assessment was unsentimental. These solutions will appear anyway.

This produced the sharpest exchange of the seminar. A Swiss participant pressed the point. The system works a thousand times and fails on the thousand and first. What then? The answer, as matters currently stand, is that whoever deploys it is liable. The Swiss response was that this is not an adequate answer, and that one cannot claim trust and then assign the consequences entirely to the user. Nortal's counter-position is the genuine insight. They are not proposing these tools, and the tools appear regardless, so the answer must lie in service design, through additional verification layers and notifications for actions taken by agents rather than humans. As Liivak put it, if he submits his company taxes in person, he does not need a notification telling him he has just submitted his taxes. If an agent does it on his behalf, he might. And for that to work, the service has to know it was an agent, which with current services is not possible.

Two observations from the same discussion are worth carrying into Swiss deliberations. Agents require more explanation than humans, not less, because they lack lived context. And the trust relationship runs in both directions: the state must know that the citizen granted the consent and that the agent genuinely belongs to the provider it claims, but the agent must equally be able to verify that something which looks like the tax authority actually is the tax authority. Estonia is actively debating what it calls AI residency, meaning the assignment of a legal identity to an agent, tied to an owner and a set of rights. As the e-Estonia Briefing Centre acknowledged, no country in the world has yet worked out how to grant permissions to AI agents. The incentive design under discussion is elegant. Registered agents would receive additional protection, in that certain actions become revocable, so that an error by a registered agent can be reversed whereas an error the citizen made personally cannot.

Helmes, founded in 1991 as the first IT company in re-independent Estonia, supplied the necessary counterweight to enthusiasm. Its Chief Innovation Officer offered a reference point that should be read carefully by anyone who has approved a large digitalisation budget. Helmes built the world's first state e-prescription platform.

Finland began five years earlier and finished five to ten years later. The Estonian system took roughly one year, a team of five to ten people at peak, and under one million euros. The challenge, he said, was not technological. What nearly caused it to fail was the coordination of government, registers, hospitals, pharmacies and software providers, some of whom actively worked against it. Almost no project fails because of technology, only because of inefficient cooperation. At kick-off he therefore asks stakeholders directly whether they want the initiative to succeed, whether they have the time, and whether they have the competence. In his experience, every second time there is someone in the room who does not want it.

On artificial intelligence specifically, Helmes identified a bottleneck that is systematically overlooked. The domain expert who must supply the input is the same person who must verify the output. Produce ten times the volume and that person is worse off rather than better. The bottleneck moves. It does not disappear. Their senior AI consultant added a qualification framework applied in a deliberate order: first business value at scale, then a business champion with support from legal, compliance and data protection, then sufficient data of sufficient quality, and only then technical feasibility, which is rarely the obstacle. At one client, fifteen to twenty ideas produced three deep dives and a single initiative taken forward. And against the escalation of sunk cost, his advice was the most practical sentence of the week: *"Be bold. Cut the cord as fast as possible. Even if the market is telling you you will be left behind, you will not be."*

3 What Switzerland Can Take Home

The delegation was told repeatedly that Switzerland and Estonia want the same things and navigate differently. Eight proposals follow from what was seen.

1. Treat the e-ID as national infrastructure rather than as a product. The Swiss honorary consul in Estonia, who has observed the Estonian system for twenty-five years, made the case directly. Electronic identity should be built and funded like roads, publicly financed, useful to everyone, and free or nearly so at the point of use. Revenue comes later from the services built on top of it.

2. Do not deliver the e-ID solely as a smartphone application. Estonia offers card, USB token, SIM-based and app-based options. The warning was explicit. An app-only token discriminates against desktop users, and it is quite likely that desktop workers are far heavier users of an electronic identity than those swiping through social media.

3. Find the Swiss equivalent of the transport discount. Estonia's card was unpopular for six years. What changed was not a campaign but visible utility, first a discount for registering a public transport pass with one's personal code, then access to online banking. An identity credential becomes popular when it saves people money or time, not when it is explained to them.

4. Build the legal and organisational layers alongside the technical one. A data exchange platform without legally equivalent digital signatures produces a portal. Signature legislation without names, accountable register owners and a binding once-only principle produces an instrument nobody uses. Switzerland's federal structure is not an obstacle. Cantons and municipalities can retain ownership of their data and systems while the federal level mandates a standard for secure exchange.

5. Adopt transparency with consequences. Estonian citizens can see who accessed their data and when. That is only meaningful because unauthorised access has real consequences, as in the 2012 case, where every person who accessed a patient record out of curiosity was dismissed. Transparency without enforcement is theatre.

6. Consider normalising incident disclosure. Estonia's deliberate strategy is that the public should expect to read about incidents, so that silence rather than disclosure becomes the cause for concern. This inverts the standard official reflex and merits serious examination in Switzerland.

7. Bring Swiss expertise into Locked Shields. A member of the delegation who has attended the exercise observed that it trains the defence of power grids and the prevention of website defacement, while Swiss companies lose money when an adversary reaches their data, from hardened data centres down to the device under a small business owner's desk. Switzerland has deep expertise in exactly that. The Centre's response was concrete and actionable. Proposals go to the exercise team well in advance, since the following year's plan is fixed by late summer, and a document with 55 options is circulated to member nations for prioritisation. The binding constraint is the availability of a digital twin. Switzerland has a National Representative at the Centre and a representative on its steering board, so this is a channel the Alliance could use within weeks.

8. Begin post-quantum migration on the assumption of 2030 rather than 2040. The estimated qubit requirement for breaking RSA fell from twenty million to one hundred thousand in six years, and Google targets internal readiness by 2029. Even allowing for the scepticism of the algorithm's own author, the planning horizon for Swiss critical infrastructure should assume the earlier date. Encrypted traffic intercepted today can be decrypted later.

4 Conclusion

The mechanism behind everything the delegation saw was described almost in passing, at the very end of the last visit. Estonia's head of CERT joined last year from cyber command. The head of the national cyber security centre came from an internet service provider. The people who built CERT now work at the company that hosted the delegation the previous evening.

"It's the same community. We try our hardest to keep the community together. I think that's the success for such a small country. You cannot be obscure. You have to be open; you have to talk with everybody. And if you're bad at the job, it's going to show soon."

In a small country, reputation is the enforcement mechanism. Neither Finland nor Estonia has any structural advantage Switzerland lacks. Both have less money, fewer people and more difficult neighbours. What they have instead is the habit of deciding things together and then living with the decision, whether the subject is a nuclear repository, a mandatory identity card or the publication of an incident nobody was obliged to disclose. That habit is a condition Switzerland shares, and it may be the most transferable asset of all.

5 Acknowledgements

Alliance Digital Security Switzerland ADSS extends its sincere thanks to all hosts and speakers for their time, expertise, and openness throughout the seminar: VTT Technical Research Centre of Finland, ICEYE, IQM Quantum Computers, the e-Estonia Briefing Centre, Helmes AS, Nortal, RaulWalter, the NATO Cooperative Cyber Defence Centre of Excellence (CCDCOE), and the Estonian Information System Authority (RIA).

Particular thanks go to Andres Sutt, Minister of Energy and the Environment of the Republic of Estonia, for addressing the delegation at the Tallinn conference; Sophie Steiner Kernen and the Swiss Embassy in Finland, as well as the Swiss Embassy for the Baltic States; Andreas Lehmann, Swiss Honorary Consul in Estonia; Mirjam Loertscher of the Estonian Ministry of Foreign Affairs, whose invaluable support helped make much of the Estonian program possible; Gustav Henriksson of Switzerland Global Enterprise; and Philipp Jordi of the Ministry for Foreign Affairs of Finland.

We are also deeply grateful to our seminar sponsors and partners — Amazon Web Services Switzerland (AWS), Helmes AS, and ICPRO — whose generous support contributed significantly to making the seminar possible.

Special recognition goes to the seminar co-leads, Dr. Elisabetta Depace and Andreas W. Kaelin, whose joint leadership shaped the program, guided the delegation, and connected the discussions and experiences across Helsinki and Tallinn.

Finally, our heartfelt thanks go to Stefanie Maurer for documenting the seminar through her photography and for the graphic design of the seminar booklet.

Explore the full seminar program and learn more about the organizations, speakers, and topics that shaped our journey through Finland and Estonia.

6 References

NATO Cooperative Cyber Defence Centre of Excellence, *Locked Shields 2026 united the power of 41 nations to defend cyberspace*, Tallinn, April 2026.

Posiva Oy, *STUK's safety assessment takes the world's first final disposal facility closer to an operating licence*, press release, August 2026.

ICEYE and Rheinmetall, *ICEYE and Rheinmetall win major contract worth billions for space reconnaissance*, press release, 18 December 2025.

North Atlantic Treaty Organization, *Wales Summit Declaration*, 5 September 2014.

Directive (EU) 2022/2555 of the European Parliament and of the Council on measures for a high common level of cybersecurity across the Union (NIS2).

e-Estonia Briefing Centre, *Interoperability Services: X-Road*, Tallinn.

Author: ***Florian Muff, Member of the Board, Alliance Digital Security Switzerland.***
Figures and quotations are drawn from presentations and discussions during the seminar of 29 August to 3 September 2026 and, where indicated, verified against public sources.