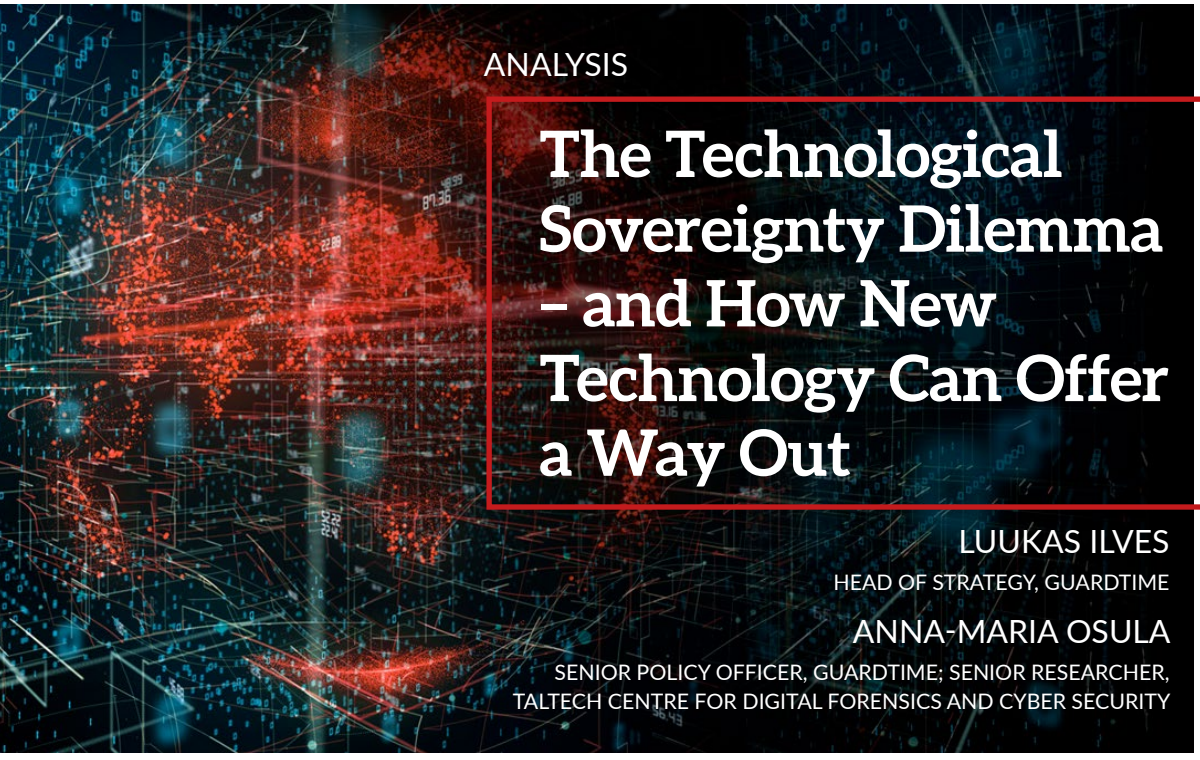


ANALYSIS

The Technological Sovereignty Dilemma – and How New Technology Can Offer a Way Out

LUUKAS ILVES
HEAD OF STRATEGY, GUARDTIME

ANNA-MARIA OSULA
SENIOR POLICY OFFICER, GUARDTIME; SENIOR RESEARCHER, TALTECH CENTRE FOR DIGITAL FORENSICS AND CYBER SECURITY

Over the past two decades, digitalisation has become the primary driver of globalisation and cross-border economic integration. New technologies and economic models promise to enable further integration in the coming decades. However, with geopolitical rivalry growing across the world, this open integration may have run its course. This article discusses how disruptive technology and "autonomy by design" may solve some of the technological sovereignty issues faced by the EU.

Governments across the world are making digital autonomy and sovereignty core parts of their economic, security, and diplomatic strategy, often at significant cost. The US-China digital "trade war" over 5G networking technology and mobile software that has been unfolding over the past year is the newest flashpoint.[1] And the new European Commission is putting Europe's "technological sovereignty" at the centre of its strategy for the next five years[2]

Behind this concern is a structural tension between the integrated nature of the global digital economy and the enduring responsibility of any sovereign government for security and domestic rule of law.

1 Fearing that equipment from Chinese manufacturers could serve as a Trojan horse for exploitation of its critical infrastructure, the US has effectively banned Huawei and other Chinese equipment from the core of its domestic 5G networks and encouraged its allies to take similar steps. Alarms have similarly been raised about Chinese tech companies doing the bidding of their government abroad (for instance taking down posts in the US about pro-democracy protests in Hong Kong). China, for its part, effectively bans many US cloud services from operating in China through its great firewall. Chinese companies have been working to reduce their dependency on US technology in everything from operating systems to chips.

2 Europe's push for technological sovereignty began in earnest after allegations in 2013 of large-scale espionage by US intelligence services. Since then, several steps have been taken that point at the need for more autonomy, such as changing EU competition rules to favour European stakeholders, setting up an EU-wide payments system and discussions on new rules on digital taxation. Domestically, individual Member States have come up with options for alternatives to huge US cloud service providers. The new President of the European Commission, Ursula van der Leyen, specifically called for pursuing "technological sovereignty" in her inaugural agenda: https://ec.europa.eu/commission/sites/beta-political/files/political-guidelines-next-commission_en.pdf

No doubt, this problem is here to stay: the next generation of digital technologies and economic models will only highlight the issue.

Policy-makers' existing toolbox is not up to the challenge. Many current and proposed technological sovereignty measures force governments into a difficult and costly trade-off between taking advantage of the benefits of digital technologies and surrendering control. The ideas behind "security by design" provide an answer – we need products and services that enable a level of trust and verifiability functionally superior to what sovereign control promises. The good news is that the tools to solve this problem are available, waiting for governments and companies to broadly adopt them: new technologies and measures of transparency, audit, and control will enable governments and users to verify how their technologies and services are behaving and allay concerns over compromise and attack.

Many current and proposed technological sovereignty measures force governments into a difficult trade-off between taking advantage of the benefits of digital technologies and surrendering control.

The technological sovereignty problem

Policy-makers have good reasons to be worried about technological sovereignty and autonomy in the Internet era. Technologies connected to the Internet and new emerging business models have changed the way our societies function and are affecting relationships between states. Three main factors – dependency, concentration problems, and cross-border character – play a role in reshaping governments' policies towards digital autonomy. While this problem is global, we will focus in particular on the European dimensions of technological sovereignty.

Firstly, we have become more dependent on digital technologies. The "digital economy" is equivalent to 15.5% of global GDP and has grown two and a half times faster than global GDP over the past 15 years (Huawei, 2017). In many industries, new entrants are disrupting long-standing incumbents. As cyberspace is increasingly also used for malicious purposes, countries' interest in controlling cyberspace has spiked.

Three main factors – dependency, cross-border character, and concentration problems – play a role in reshaping governments' policies towards digital autonomy.

Secondly, this digital transformation is shaping up to be a winner-takes-all phenomenon, with category-leading companies able to offer their products and services on a global scale. This allows them to reap economies of scale and spread innovations into all markets. The biggest technology platforms – now the world's most valuable companies – are offering essential digital infrastructure on a global level, frequently leaving no viable domestic alternative.

Finally, as jurisdictional boundaries begin to blur in cyberspace, the conventional territorial foundations of sovereignty are no longer as solid as they used to be. In the context of criminal investigations, service providers such as Google and Facebook are now required (under both the US CLOUD Act and the proposed EU e-Evidence framework) to share specific data with domestic and international law enforcement offices irrespective of the actual physical location of the data. This is a significant change from the previously prevalent "territorial" approach where data location was the main determining connecting factor to identify the foreign state with whom to initiate the Mutual Legal Assistance process in order to obtain access to the evidence (e.g. Osula, 2017).

It does not stop with digital evidence. The effective nexus for controlling large swaths of how a society functions – transport, housing, energy, health, food, financial services – is coming unmoored from the territorial jurisdiction where the service is provided, with the service provider subject to orders from their headquarters' home country or a third country. Further developments such as cryptocurrencies threaten states' classical monopolies in domains like monetary, taxation, and social policy.

The most capable and committed governments are keen to exploit their "cyber power" as a new form of power projection, sometimes employing companies under their jurisdiction and control as their agents. While their intentions can be benign and their actions can even seem necessary in a globalised world – e.g. the pursuit of terrorists or money laundering – such activity leaves most countries suffering from a "sovereignty gap" and concerned about domestic rule of law (Schaake, 2017). This is a gap new policies of technological sovereignty and autonomy are intended to fill (Nye, 2010; Kello, 2018).

There are two technological and economic trends which will have an effect on how governments are able to deal with further digitalisation.

The first of these – "software-defined everything" – describes the idea that computers now run everything, including the physical environment around us, from car brakes and door locks to factories and supply chains, complex transportation and energy systems. What was previously hard-wired or coded is now constantly modifiable, updateable, hackable – and, in effect, a black box for those who would certify or inspect the functioning of a device. And general-purpose machines replace specialised equipment (e.g. the smartphone, which functions as a GPS receiver, calendar, map, radio, telephone, metronome and piano tuner, voice recorder, camera, measuring tape, pedometer, sports watch, digital identity/smartcard, etc.).

The second – "servitisation" – describes companies moving toward offering services in lieu of products (for an exploration of the idea, see Osimo & Ilves, 2019: 28–29). Software-as-a-service is the prime example: Gartner predicts that by 2020, 80% of software will be subscription-based (Gartner, 2018). However, this extends well beyond digital products: Rolls Royce has introduced new "pay by the hour" models for its airplane engines, instead of the equipment itself, while car manufacturers are preparing for an era where individuals no longer buy automobiles but consume "mobility-as-service". Instead of purchasing a clearly defined good, customers enter a long-term relationship with their supplier and consume a product that is constantly being updated and changed.

The most capable and committed governments are keen to exploit their "cyber power" as a new form of power projection, sometimes employing companies under their jurisdiction and control as their agents.

Both of these trends exacerbate technological sovereignty challenges: the service you subscribe to today could change tomorrow, the software of your certified device can be reconfigured in minutes with an over-the-air update. This is generally a good thing, enabling convenience, responsiveness, quality, and continuous improvements. But this also opens a window – for malicious cyberattackers, including foreign governments – to reach straight into a country's critical infrastructure, sensitive data, and overall economy.

Toolbox

The terms "strategic autonomy" and "technological sovereignty" have become a catch-all for measures to limit exposure to these risks. Governments are considering a broad policy toolbox, with measures generally intended to increase government control or promote domestic competitors.

Common proposals include (Leonard et al., 2019; Aaronson, 2018):

- industrial policy and domestic technology development programmes, including in new technologies such as 5G, AI, quantum computing;
- rules to limit foreign companies (e.g. rules on foreign ownership) or indirect measures (such as taxation and competition rules);
- preference for domestic technologies and services, expressed in procurement or legal requirements;
- forced localisation (e.g. data localisation, requirements for local staff or headquarters) or filtering and blocking non-domestic data and services;

- more aggressive jurisdictional concepts or universal jurisdiction, e.g. the US CLOUD Act and the EU GDPR and the proposed e-Evidence regulation;
- stronger cybersecurity rules and capacity, notably reporting, information sharing, and standards;
- "security by design", e.g. requirements for testing and standardisation, opening source code for review.

This toolbox lays out the dilemma posed by "technological sovereignty": measures that increase domestic control over technology have serious costs. Technological autarky and even simple localisation rules break global supply chains. New legal requirements create compliance costs also for domestic firms (e.g. Hohmann et al., 2014). Industrial policy can lead to costly technology choices. And *other countries'* policies can hurt one's own firms. At worst, we risk escalating *beggar-thy-neighbor* policies leading to widespread "digital protectionism" and mercantilism (Denton, 2019). Studies of just one such practice, forced data localisation, have pegged the cost of current and proposed measures at 1% of global GDP (see Bauer et al., 2014; Bauer et al., 2016).

Perhaps the biggest cost of limiting foreign technology and services is its impact on broader technological adoption. The ICT industry itself forms narrowly 4–8% of the economy in most countries (see OECD indicators). Economic success comes from the speed with which the economy digitalises (and raises labour productivity) as a whole. Tomorrow's digital leaders will be those who aggressively use today's technology. Conversely, measures that make new technology harder or more expensive to use harm countries' broader digital agendas.

This toolbox lays out the dilemma posed by "technological sovereignty": measures that increase domestic control over technology have serious costs.

The European Commission's internal think tank summarises the dilemma of technological sovereignty:

> [I]n today's interconnected world of globalised supply chains, no one can walk alone. From a strategic point of view, the issue is hence more complex than simply seeking to prevent, or eliminate, vulnerabilities in supply chains. In many respects, it appears more realistic to find ways to manage and reduce, when possible, these vulnerabilities. Likewise, some dependencies might be less critical than others, depending on the country of origin and the technologies involved (EPSC, 2019: 10).

Three core technologies (5G, Cloud, and AI) illustrate the tradeoffs behind the technological sovereignty dilemma and the challenge posed by the increasing pervasiveness of software- and services-driven offerings.

5G is the newest generation of mobile broadband technology, currently being rolled out across the world. Like 2-3-4G before it, 5G will bring faster mobile broadband, but its transformational effect arises from other characteristics – low latency and low power connections that will bring mobile connectivity to billions of IoT devices, from construction equipment and autonomous cars to small transmitters in clothing, medical equipment, and household goods. And along with this connectivity come all the risks of connected devices.

5G equipment relies on "software-defined" networking and radio equipment to handle the massive volumes and variations in the use cases the technology allows (Routray, & Sharmila, 2017). This in turn can only be accomplished through frequent updates and active management of the network by the manufacturer (European Commission, 2019). Traditional controls – thorough examination and certification of hardware and software before deployment – fail to effectively address this active management. In these circumstances, the US government determined that it could never be sure it could prevent the Chinese government from exploiting the presence of Huawei equipment in networks, and chose an outright ban on Huawei equipment as the most expedient solution (for a summary of US Government considerations: Defense Innovation Board, 2019). Other governments are arriving at similar conclusions.

This choice, however, carries significant costs. In the short term, many experts conclude that Huawei offers the operationally most effective (and cheapest) end-to-end solution for deploying 5G (GlobalData, 2019). In its absence, the market is basically confined to two providers, with limited competition potentially raising the cost of 5G (Barzic, 2019). Furthermore, a policy of excluding Huawei from 5G networks also requires previous equipment investments to be recouped, at a cost of billions of euros in the EU alone.[3]

Cloud computing, narrowly construed, is a service that facilitates the on-demand availability of computer system resources. But the promise of cloud computing goes beyond providing a more efficient infrastructure: enterprise functions that were previously provided in-house (e.g. human resources, accounting, training, internal and external communications, business intelligence, quality assurance, specialised services from monitoring aircraft engine performance to detecting financial crime) can now be consumed as cloud services (Bommadevara et al., 2018).

Today, the productivity benefits of digitalisation are delivered via cloud, which is also the easiest way to consume new technologies like AI and Blockchain without requiring specialised staff or major upfront investments. This disrupts the scale advantage of large firms and makes it easier for a startup or small business to scale rapidly.

European concerns about cloud computing highlight the sovereignty dilemma. European firms already lag significantly behind their American counterparts in adopting cloud services (Targett, 2018). Partly as a result, Europe also has far fewer cloud and software-as-a-service startups (e.g., Eurostat, 2018; Lorica & Nathan, 2018).

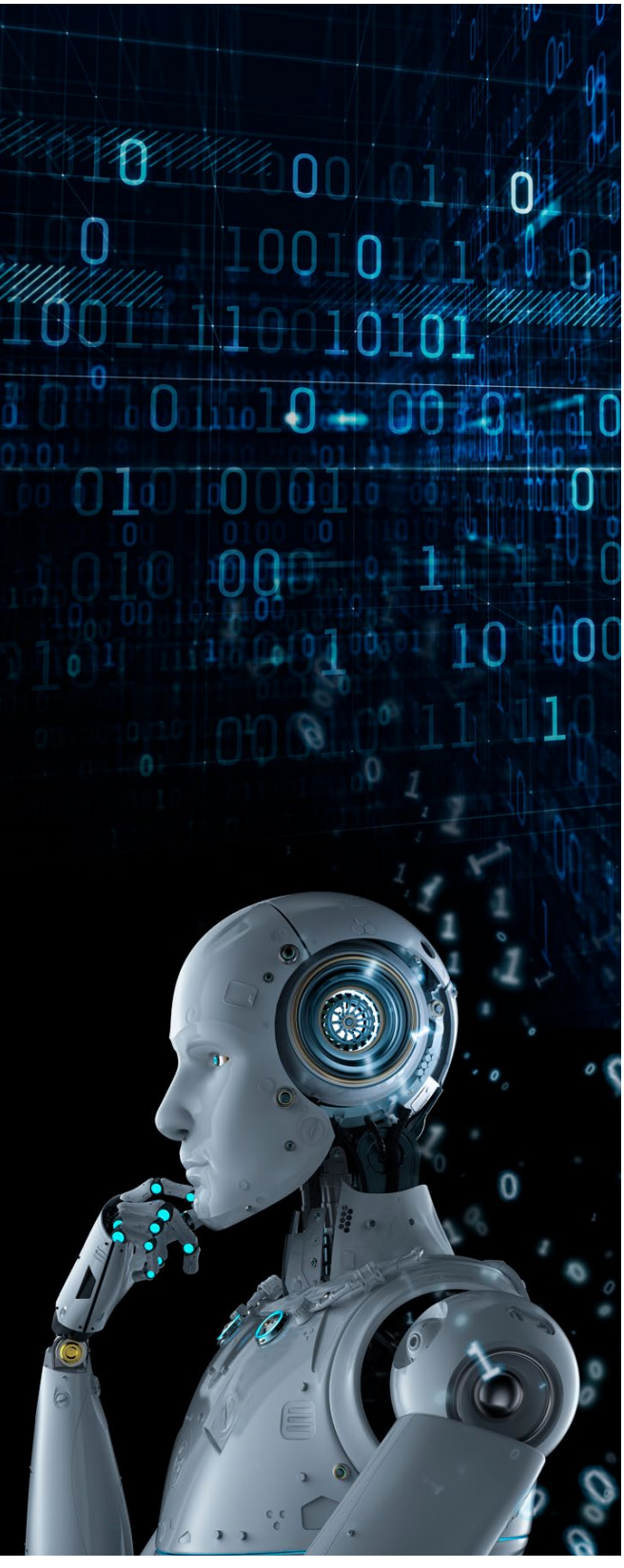
Data sovereignty concerns are leading European governments to launch costly new initiatives for cloud infrastructure that do not necessarily address the adoption question. Partly in response to the US CLOUD Act, which would allow the US federal law enforcement officers to demand data from the servers of American tech firms located anywhere in the world, the French and German government launched the "Gaia-X" project. Due to be established in spring of 2020, the initiative is a response to the "European economy urgently need[ing] an infrastructure that ensures data sovereignty" (Meyer, 2019). The infrastructure will be developed in cooperation with France and a number of private sector actors, and further activities will include establishing data warehouses, data pooling, and developing data interoperability. At the same time the EU is lacking a uniform approach in this question. For instance, in 2018 the Polish government launched the programme "Common Information Infrastructure of the State" which also includes setting up a "Public Computational Cloud" in cooperation with Google (Operator Chmury Krajowej, 2019).

The development of Artificial Intelligence has surged forward in the past decade. Driven by massive increases in data and computing power (via cloud computing), machine learning (ML) is enabling large swaths of human tasks to be automated, with major economic and social consequences.[4]

Using AI is a bit like hiring a person, requiring trust in a black box we cannot fully control. Tools built on ML and associated technologies are not static; their functionality is constantly evolving based on new data and learning cycles. They must be configured and set up properly to work well.

3 The only form of 5G networks that can currently be deployed by telecom operators are "non-stand-alone" – built on top of existing 4G networks by the same manufacturer. For telecoms operators whose 4G equipment is built on Huawei – including many in Europe – the choice not to use Huawei equipment for 5G networks means either waiting several years before deploying 5G or a bill in the hundreds of millions or in billions to replace significant components of their 4G network before they even begin 5G deployment. See GSMA, 2019. See also the balanced risk-based approach provided by the EU 5G toolbox, European Commission, 2020.

4 It is estimated that AI will add $15.7 trillion to the global economy by 2030. At the same time, 15 percent of the global workforce – or about 400 million workers – could be displaced by automation. As in the case of 5G and cloud, the greatest returns will come from broad adoption of AI technologies across different economic sectors.



And – in the case of many deep learning models – their internal functioning is effectively a black box that even the designers of the specific algorithm cannot fully explain.[5] Traditional approaches to testing and certification cannot track a dynamic system. Systems that use AI become unpredictable and can often produce unexpected effects – leading to the broad and far-reaching discussion on the ethics and human rights impacts of AI as well as design principles for safe, secure and reliable AI (Ilves, 2018).

Most cutting-edge applications of AI are being designed in the US and China, with core components provided by a limited number of companies, such as Google's Tensor Flow and IBM's Watson, increasingly baked into most enterprise AI products. We are seeing increasing concern about the provenance and trustworthiness of AI, analogous to existing discussions around Cloud and 5G (e.g. Renda, 2019). The dilemma policy-makers face will be similar – building a set of sovereign technologies while excluding US or Chinese technology on the grounds of national origin may be the only reliable way to address all trust concerns around a foreign-sourced technology, but doing so will come at immense cost – including possibly slowing down one's own industrial and economic progress by years.

Security and autonomy by design

The notion of "security by design" points to a way out of the technological sovereignty dilemma. If we can design our digital products and services so as to preclude misuse and guarantee that services perform as promised, we can eliminate much of the risk that policies for technological sovereignty are trying to address. Effective control over the ongoing functioning of a product or service can make up for foreign provenance or control over the service provider. Ultimately, "security by design" should deliver "autonomy by design".[6]

5 While there is significant research in the area of "explainable AI", it has thus far not satisfactorily addressed the question.

6 To be sure, "security by design" measures cannot address all technological sovereignty concerns. Notably, they are silent on the question of reliability and do not reduce the industrial costs of long-term dependency on foreign suppliers. But they do give policy-makers more leverage, allowing them to focus on developing domestic technologies and supply chains in a more targeted manner.

The EU has steadily worked on enshrining the principles of "security by design" (and its cousin, "privacy by design") in its legislative frameworks. For example, the new EU Cybersecurity Act establishes cybersecurity certification schemes which play an important role in enhancing trust and security in products, services, and processes by encouraging manufacturers or providers involved in their design and development to implement security measures at the earliest stages of design and development (EU Regulation 2019/881: Art. 13). The EU's data protection rules (the GDPR) also clearly underline the relevance of "data protection by design and by default" (EU Regulation 2016/679: Art. 25). Other measures include adopting security standards, the use of ethical hacking and penetration testing for ensuring the security of the products, services, and processes as well as putting in place requirements for an assured supply chain (e.g. Eurosmart, 2019).

"Security by design" points to a possible way out of the technological sovereignty dilemma.

However, current approaches to security by design suffer from significant limitations that keep them from reaching the level of control technological sovereignty concerns demand:

- Security testing, certification, penetration testing, and auditing are expensive and labour-intensive. This approach will struggle to scale broadly.[7]
- They focus on initial design of a product or service, not the ongoing and dynamic processes that are common in the digital world today. Common practices in software engineering and service design, including extensive multi-party supply chains and continuous updates, break this paradigm (as described above for 5G and cloud). One software update and new release later the product may have changed entirely.
- Auditing and testing alone simply move the trust and provability burden elsewhere, to the question of "do you trust your testing lab or auditor?" "Security by design" will not solve our digital sovereignty dilemma if products and services still need to comply with multiple different standards and be audited, testified, or certified in each country they are used in.
- Many (in principle) highly secure systems are compromised because of user error in configuration and setup. Any approach to solving the technological sovereignty dilemma that relies on technology must also work in the real world.

However, new technologies and approaches can address these shortcomings to the point where many of the control questions raised in this article can be convincingly addressed. "Autonomy by design" relies on three fundamental functionalities to ensure that technology and its uses are free from outside influence: scalable data and process integrity, automated testing, and transparency. New trust technologies (e.g. blockchain) and forms of automation (e.g. AI) now make these realisable in practice.

1) Scalable data and process integrity[8]

Data integrity is a fundamental aspect of information security that deserves more attention in the context of security by design. The integrity of individual data objects is central to a wide variety of trusted processes, from log analysis to elections. And the stakes are rising: automated processes that rely on exponentially growing volume and speed need to be able to verify the integrity of their input in real-time.

How do I know, in real time, that my 5G base station, autopilot, or cloud service have not been compromised by the manufacturer or a third party? Can I prevent the risk scenarios described in this paper?

This entails proving a negative – that no compromise of the system has occurred. Reaching a sufficient level of proof means real-time tracking,

7 For instance, a regular penetration test costs anything between $15,000 and $30,000, while comprehensive audits can cost hundreds of thousands. See Tritten, 2020; Glover. For a list of Conformity Assessment Bodies, see ENISA 2019.

8 Within the narrow context of information security, the term integrity means to protect the accuracy and completeness of information, see ISO standard (ISO/IEC 27000, 2014: section 2).

logging, and reporting millions of steps in complex processes, often over multiple computing environments, while generating cryptographic proof of this process. There are now scalable forms of blockchain technology in use in industrial applications, including in the US defence supply chain and mission critical industries such as shipping, that reach this standard (Linkov et al., 2018, Vestergaard & Umayam, 2019). Similar technology is being applied to cloud computing and AI training, providing process integrity at a scale sufficient for "hyper-automation", where AI systems can act directly upon insights without human intervention (Kenyon, 2019: 2). Applied to cloud computing, this means real-time awareness of what is happening to cloud-based processes on a bits-and-bytes level, ongoing confirmation that a cloud deployment corresponds to the parameters of relevant certifications, and immediate alerts and automated action if something deviates from these parameters (e.g. insider compromise or an unauthorised access based on e.g. foreign e-evidence requests).

2) Automated testing

Where services are not configured to provide ongoing proof of data and process integrity, we should aim for ongoing, scalable testing that occurs at the speed of software. AI and autonomous agents promise to automate security and compliance testing. The 2016 DARPA Cyber Grand Challenge saw automated penetration testers outperform human teams. Applied broadly, such an approach enables a wide range of security and conformity tests to be performed at scale. Automated testing can serve to reduce the risks of the black box problem presented by AI, cloud, 5G, and other new technologies. For instance, a wide variety of cybersecurity startups now promise automated cybersecurity and penetration testing to discover vulnerabilities or configuration errors and to assess the security of a product or service.[9]

As a next step, increasingly sophisticated virtualised testing environments allow new software and updates to be tested before release, but in real time. This allows testing and certification to be built into dynamic, quickly developing products and services without a significant compromise in usability or availability.

3) Transparency, accountability, and automated compliance

Of course, both process integrity and automated testing will only create confidence for policy-makers when these can be independently verified by third parties, including regulators and government cybersecurity centres.

Transparency is becoming the "new normal" both in private and public sectors. For example, the retail industry has discovered the merits of blockchain technology, allowing the consumer to track how products are sourced and providing transparency as well as traceability throughout the entire supply chain (Weinswig, 2018). Governments are also relying on providing transparency to users to engender trust in increasingly digitalised public services, especially when these involve sensitive personal data.[10] For instance, Estonia's e-health system provides an independent forensic-quality audit trail for the lifecycle of patient records, making it impossible for anyone who gains access to those records to manipulate information and cover their tracks (E-Estonia, 2016).

The last decade has also seen an explosion in region- or vertical-specific regulation centred around trust and auditability (notably around privacy and financial services). The burden of complying with these rules has spawned a new generation of services focused on simplifying and automating compliance (RegTech, short for regulatory technology). RegTech allows companies to manage and track their compliance and ultimately demonstrate to regulators that they have acted appropriately. By using automated and machine-readable reporting, compliance becomes an automated process.

Ultimately, we see a virtuous cycle of process integrity, automated testing, compliance, and accountability, providing the ability to ensure that digital

9 E.g. Aquascan, Pcysys, Security Scorecard.

10 See, e.g. the eGovernance Benchmark report showcasing the digital efforts in the EU: European Commission, 2018.

services and software function as promised.[11] These tools allow us to realise "continuous compliance", whereby ongoing conformity of a system can be ascertained second-to-second. States, regulators, and users can reach a level of control and oversight over technology and services that are not designed and developed domestically or are offered from another jurisdiction, while achieving the same or greater level of oversight and trust as they would wish for in their own sovereign technology.[12]

In expanding the toolbox at their disposal, policy-makers should actively consider how new standards of evidence, proof, and compliance could be used to make products and services trustworthy and controllable, even where they are of foreign origin.

These capabilities are underpinned by recent technological developments (scalable blockchain and AI), but we emphatically do not propose that policy-makers should therefore simply mandate the use of these technologies. The technological sovereignty concerns outlined in this paper and elsewhere arise from functional concerns over the functioning of modern IT systems. The solution, too, should be specified in functional terms. In expanding the toolbox at their disposal, policy-makers should actively consider how new standards of evidence, proof, and compliance could be used to make products and services trustworthy and controllable, even where they are of foreign origin.

This is an area that calls for EU leadership. Europe continues to be one of the largest exporters of digital goods and services (Eurostat, 2018). European manufacturers and technology companies will pay the price of the technological sovereignty dilemma, as Europe, the US, China, India, Brazil and other parts of the world impose new restrictions. Conversely, a broad adoption of "security and autonomy by design" measures would help European offerings thrive and shore up globalised, open markets. In short, the EU has good reasons to promote technological and design solutions to the technological sovereignty dilemma, both to support its own digital development at home and to set an example for the rest of the world.

11 For example, the EU's newly published toolbox for secure 5G networks covers functionalities such as strong security requirements, strict access controls, monitoring, reinforcing testing and auditing capabilities (European Commission, 2020).

12 Frequently, tools for oversight, PKI, etc. are called "trust services" and "trust technology". This name gives insight into their limitations – they entail trusting another party. And the need to trust third parties is precisely the problem that is being put under stress with arguments for technological sovereignty, which basically say that "we cannot trust all the parties potentially involved in this process or supply chain." So we need to move beyond trust to independent "truth", verified frequently and by many parties.

About the authors:

Luukas Ilves is Head of Strategy at Guardtime. For the past two years, he also chaired the Council of Europe's Committee of Experts on human rights dimensions of automated data processing and different forms of artificial intelligence. He has previously held policy-making positions in the Estonian Government and European Commission, focusing on cyber security, digital government, and data flows.

Dr. Anna-Maria Osula serves as Senior Policy Officer at Guardtime and Senior Researcher at TalTech Centre for Digital Forensics and Cyber Security. During 2008-2018 she worked as a legal researcher at the NATO Cyber Defence Centre of Excellence.

References

Aaronson, S. A. (2018). What Are We Talking about When We Talk about Digital Protectionism?. Washington, DC: George Washington University. Retrieved from https://www2.gwu.edu/~iiep/assets/docs/papers/2018WP/AaronsonIIEP2018-13.pdf

Barzic, G. (7 June 2019). Europe's 5G to cost $62 billion more if Chinese vendors banned: telcos. Retrieved from https://www.reuters.com/article/us-huawei-europe-gsma/europes-5g-to-cost-62-billion-more-if-chinese-vendors-banned-industry-idUSKCN1T80Y3

Bauer, M., Ferracane, M. F., Lee-Makiyama, H., & Van der Marel, E. (2016). Research Report Unleashing internal data flows in the EU: An economic assessment of data localisation measures in the EU member states ECIPE Policy Brief. Retrieved from https://www.econstor.eu/bitstream/10419/174802/1/ecipe-pb-2016-03-Unleashing-Internal-Data-Flows-in-the-EU.pdf

Bauer, M., Lee-Makiyama, H., Van der Marel, E., & Verschelde, B. (2014). Research Report The costs of data localisation: Friendly fire on economic recovery ECIPE Occasional Paper. Retrieved from https://www.econstor.eu/bitstream/10419/174726/1/ecipe-op-2014-3.pdf

Bommadevara, N., Del Miglio, A., & Jansen, S. (2018). Cloud adoption to accelerate IT modernization. Retrieved from https://www.mckinsey.com/business-functions/mckinsey-digital/our-insights/cloud-adoption-to-accelerate-it-modernization

Defense Innovation Board. (April 2019). The 5G Ecosystem: Risks & Opportunities for DoD. Retrieved from https://apps.dtic.mil/dtic/tr/fulltext/u2/1074509.pdf

Denton, J. (28 April 2019). Digital protectionism demands urgent response. Financial Times. Retrieved from https://www.ft.com/content/0c360404-65ba-11e9-a79d-04f350474d62

E-Estonia. (February 2016). eHealth authority partners with Guardtime to accelerate transparency and auditability in health care. Retrieved from https://e-estonia.com/ehealth-authority-partners-with-guardtime-to-accelerate-transparency-and-auditability-in-health-care

EU Regulation 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation).

EU Regulation 2019/881 of the European Parliament and of the Council of 17 April 2019 on ENISA (the European Union Agency for Cybersecurity) and on information and communications technology cybersecurity certification and repealing Regulation (EU) No 526/2013 (Cybersecurity Act).

European Commission. (2018). eGovernment Benchmark 2018: the digital efforts of European countries are visibly paying off. Retrieved from https://ec.europa.eu/digital-single-market/en/news/egovernment-benchmark-2018-digital-efforts-european-countries-are-visibly-paying

European Commission. (2019). Member States publish a report on EU coordinated risk assessment of 5G networks security. Press release. Retrieved from https://europa.eu/rapid/press-release_IP-19-6049_en.htm

European Commission. (2020). Cybersecurity of 5G networks - EU Toolbox of risk mitigating measures. CG Publication. Retrieved from https://ec.europa.eu/newsroom/dae/document.cfm?doc_id=64468

European Network and Information Security Agency (ENISA) (2019). List of conformity assessment bodies (CABs) accredited against the requirements of the eIDAS Regulation. Retrieved from https://ec.europa.eu/futurium/en/content/list-conformity-assessment-bodies-cabs-accredited-against-requirements-eidas-regulation

European Political Strategy Centre. (July 2019). Rethinking Strategic Autonomy in the Digital Age. EPSC Strategic Notes. Issue 30, July 2019. Retrieved from https://ec.europa.eu/epsc/sites/epsc/files/epsc_strategic_note_issue30_strategic_autonomy.pdf

Eurosmart. (2019). Towards European Digital Strategic Autonomy. Retrieved from https://www.eurosmart.com/towards-european-digital-strategic-autonomy-digital-sovereignty

Eurostat. (August 2018). Trends in EU trade in goods and services 2000-2017. Retrieved from https://ec.europa.eu/eurostat/web/products-eurostat-news/-/WDN-20180827-1

Eurostat. (December 2018). Cloud Computing – Statistics on the Use by Enterprises.

Gartner. (2018). Moving to a Software Subscription Model. Retrieved from https://www.gartner.com/smarterwithgartner/moving-to-a-software-subscription-model/

GlobalData. (25 June 2019). Telecom Industry's First 5G RAN Competitive Analysis by GlobalData Reveals Huawei Leaderhip. Retrieved from https://www.globaldata.com/telecom-industrys-first-5g-ran-competitive-analysis-published-by-globaldata-reveals-huawei-leadership/

Glover, G. How Much Does a Pentest Cost?. Retrieved from https://www.securitymetrics.com/blog/how-much-does-pentest-cost

GSMA. (28 March 2019). 5G Implementation Guidelines. Retrieved from https://www.gsma.com/futurenetworks/wiki/5g-implementation-guidelines/

Hohmann, M., Maurer, T., Morgus, R., & Skierka, I. (24 November 2014). Technological Sovereignty: Missing the Point? An Analysis of European Proposals after June 5, 2013. Retrieved from https://www.gppi.net/2014/11/24/technological-sovereignty-missing-the-point

Huawei. (2017). Digital Spillover: Measuring the true impact of the digital economy. Retrieved from https://www.huawei.com/minisite/gci/en/digital-spillover/files/gci_digital_spillover.pdf

Ilves, L. (October 2018). Briefing Note: Responsible, Safe and Secure AI. retrieved from https://lisboncouncil.net/publication/publication/152-responsible-safe-and-secure-artificial-intelligence.html

ISO/IEC 27000. (2014). Information technology – Security techniques – Information security management systems – Overview and vocabulary.

Kello, L. (2018). Private-Sector Cyberweapons, An Adequate Response to the Sovereignty Gap?. In: Lin, H., & Zegart, A. (Eds.). *Bytes, Bombs, and Spies*, Washington, DC: Brookings Institution Press, 2019.

Kenyon, T. (2019). Data integrity critical in securing autonomous AI. Guardtime whitepaper. Retrieved from https://m.guardtime.com/files/data-integrity-critical-in-securing-autonomous-ai.pdf

Leonard, M., Pisani-Ferry, J., Ribakova, E., Shapiro, J., & Wolff, G. B. (25 June 2019). Redefining Europe's Economic Sovereignty. Retrieved from https://bruegel.org/2019/06/redefining-europes-economic-sovereignty/

Linkov, I., Wells, E., Trump, B., Collier, Z., Goerger, S., & Lambert, J. H. (May 2018). Blockchain Benefits and Risks, Military Engineer. Retrieved from https://www.researchgate.net/publication/325385235_Blockchain_Benefits_and_Risks

Lorica, B. & Nathan, P. (October 2018). Evolving Data Infrastructure, October 2018 https://www.oreilly.com/data/free/evolving-data-infrastructure.csp

Meyer, D. (2019). Europe Is Starting to Declare Its Cloud Independence. Fortune. Retrieved from https://fortune.com/2019/10/30/europe-cloud-independence-gaia-x-germany-france/

Nye, J. (2010). Cyber power, Belfer Center for Science and International Affairs, Harvard Kennedy School. Retrieved from https://www.belfercenter.org/publication/cyber-power

OECD. Key ICT Indicators. Retrieved from https://www.oecd.org/internet/ieconomy/oecdkeyictindicators.htm

Operator Chmury Krajowej. (2019). Press release of 27 September 2019. Google Cloud został strategicznym partnerem Operatora Chmury Krajowej. Retrieved from https://chmurakrajowa.pl/partnership.html

Osimo, D., & Ilves, L. (2019). Roadmap for a Fair Data Economy. Retrieved from https://lisboncouncil.net/publication/publication/155-a-roadmap-for-a-fair-data-economy-.html

Osula, A.-M. (2017). Remote search and seizure of extraterritorial data. Tartu: University of Tartu Press.

Oxford Economics and Huawei. (December 2019). Restricting Competition in 5G Network Equipment: An Economic Impact Study. Retrieved from https://resources.oxfordeconomics.com/hubfs/Huawei_5G_2019_report_V7.pdf

Renda, A. (February 2019). Artificial Intelligence: Ethics, governance and policy challenges. Retrieved from https://www.ceps.eu/system/files/AI_TFR.pdf

Routray, S. K., & Sharmila, K. P. (2017). Software defined networking for 5G. 4th International Conference on Advanced Computing and Communication Systems (ICACCS). Retrieved from https://ieeexplore.ieee.org/document/8014576

Schaake, M. (2017). Europe should give meaning to the rule of law online. Retrieved from https://marietjeschaake.eu/en/europe-should-give-meaning-to-the-rule-of-law-online

Targett, E. (2018). Just 26% of European Enterprises Are Using the Cloud: Eurostat Report. CBR. Retrieved from https://www.cbronline.com/news/european-cloud-adoption

Tritten, T. (15 January 2020). Defense Contractors to Face Added Costs with Cybersecurity Audit. Bloomberg Government. Retrieved from https://about.bgov.com/news/defense-contractors-to-face-added-costs-with-cybersecurity-audit/

Vestergaard, C., & Umayam, M. L. (November 2019). The Prospect of Blockchain for Stengthening Nuclear Security. IAEA Conference Paper. Retried from https://conferences.iaea.org/event/181/contributions/15812/attachments/8478/11247/FINAL_Prospect_of_Blockchain_for_Strengthening_Nuclear_Security_-_27_Nov_2019.pdf

Weinswig, D. (2018). Transparency Is the New Normal: Top Takeaways from the 2018 Innovation Series. Forbes. Retrieved from https://www.forbes.com/sites/deborahweinswig/2018/05/25/transparency-is-the-new-normal-top-takeaways-from-the-2018-innovation-series/#4636a71a1e85