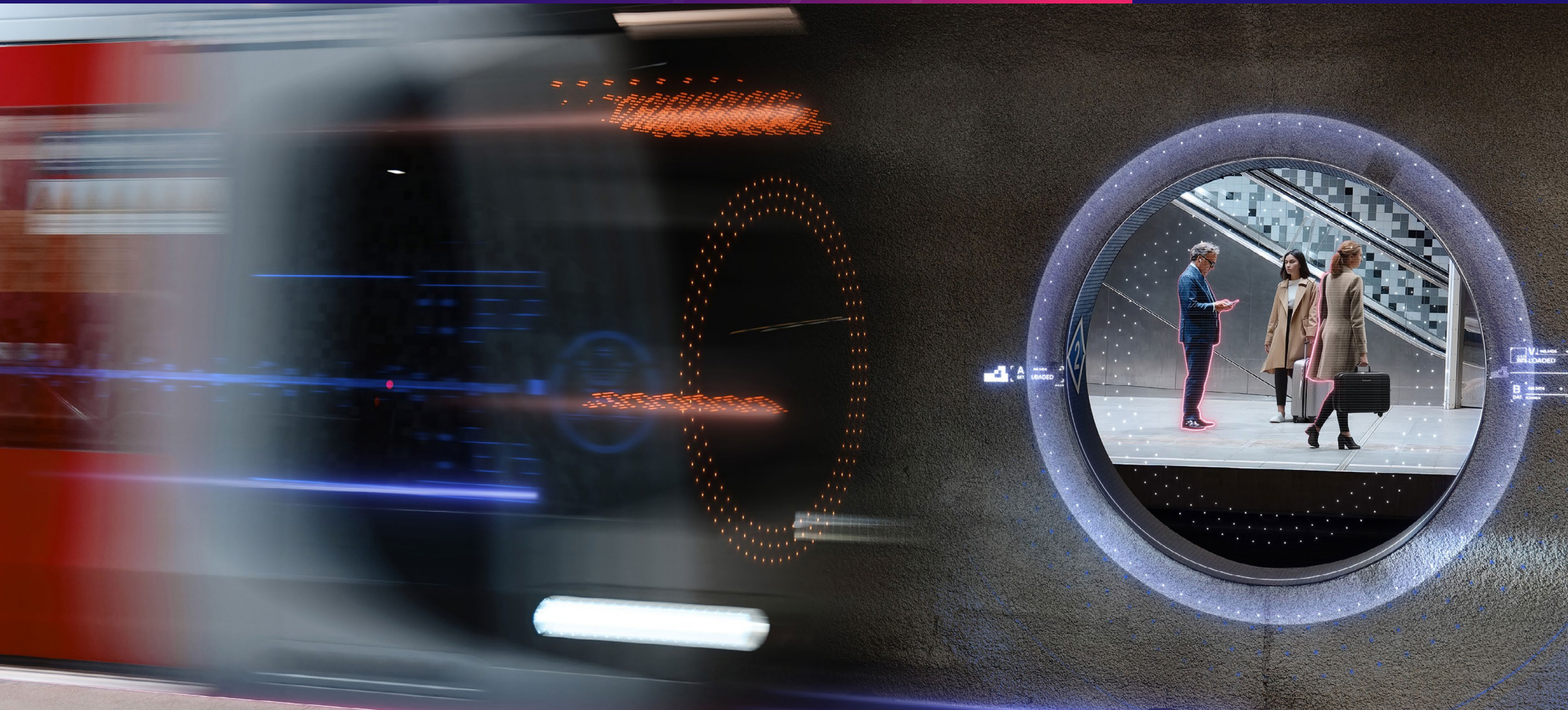
Paper

Resilient systems

On how we have to use digital technology to strengthen the resilience of our society and economy

TNO Vector
Centre for Societal Innovation and Strategy



Contents

This paper is part of a series of papers written for the 2025 TNO Vector Symposium: De kracht van samenwerkende systemen – Sturen naar een vitale, competitieve en veilige samenleving.

The goal of this paper is to provide additional insight to participants on the subject of discussion.

1. Introduction

Resilience has been a hot topic in recent years not only for policymakers, economists and business leaders, but also for society at large. Climate change, global migration, the COVID-19 pandemic and the Russian war of aggression against Ukraine are just a few examples that provide us with an image of **global instability**. The April 2025 power outage across Spain and Portugal has shown us once more how vulnerable and dependent our modern societal and economic systems are (Henley et al., 2025). Whether such disruptions are caused by natural events, human error or malicious attacks – their effect on our society and economy remains the same.[1]

At the same time, these uncertain times also provide us with **an opportunity to reflect, reprioritise and redirect our efforts** to face the challenges of today and tomorrow. Managers are changing their business models and talent development strategies in light of the ongoing AI evolution (Duke, 2025), academics are researching how organisations and government can stay on top of societal and economic transitions (Pisa et al., 2024)[2], and policymakers are reassessing the value of global alliances, shifting their strategic focus toward strengthening regional and national capabilities (Damen, 2022).

In a political landscape that is undergoing constant change, being resilient becomes ever more important – not only as an individual, but also at a system level. Recognising this need, the European Union (EU) has established Resilience Dashboards to monitor and provide insights into the resilience of individual EU Member States, with the underlying aim of improving policy decision-making (European Commission, 2020). One key domain monitored by the EU is **digital resilience**.[3] Digital technologies are omnipresent in our society and economy today. They help to accelerate economic growth and form the basis of most of our social and economic transactions. At the same time, we are heavily dependent on them, as they have become interwoven with our societal and economic systems.

This paper explores just how dependent our societal and economic systems are on digital technology, what it means for our resilience from a strategic point of view and what measures have been and should be taken to **reduce the associated risks** – and what individual leaders and organisations can do today to prepare for future uncertainty. By improving digital resilience, we can improve the resilience of our societal and economic systems – and thereby **increase our economic competitiveness and broad welfare**. As a case study, the paper looks at the financial sector, but the observations and recommendations are of general nature.

1 To resolve any misunderstanding: this is not to imply that all the listed examples (climate change, global migration, etc.) have the same effect on our society and economy, but about making a distinction between the *impact* of a disruption (e.g. a power outage) and its *cause* (e.g. human error). From a resilience perspective, the cause is often less relevant than the actual impact of an event, as the impact is what needs to be managed once a disruption has occurred.

2 See also the 2024 Vector Symposium *Strategische Autonomie in een Open Economie.*

3 For an overview of indicators and digital resilience levels of EU Member States, refer to Annex I.

2. Resilient societal and economic systems: the role of digital resilience and digital sovereignty

Our society and economy are heavily dependent on digital technologies. Whether it is digital payment systems, digital control of operational technology for water management, or digital monitoring of health data – **there are hardly any systems today that do not rely on digital technology** at least to some extent, directly or indirectly. Our wellbeing, economic competitiveness, safety and security depend on it.

A standard definition of resilience in the context of digital technology systems refers to "the ability to prepare for and adapt to changing conditions and withstand and recover rapidly from disruption," whether caused by "deliberate attacks, accidents, or naturally occurring threats or incidents" (Ross et al., 2021). We can apply this definition to other systems as well, including societal and economic ones.

In essence, **resilient systems have three inherent properties**:

- Resilient systems can adapt quickly to changing circumstances.
- In adverse situations, resilient systems can still function at a minimum necessary level.
- If a resilient system is disrupted, it is able to recover quickly.

Achieving resilience is a task difficult enough for any system, especially because of the complexity of most systems. The more complex a system, the more difficult it is to predict its behaviour and to make relevant decisions. This problem gets worse if we consider the **links between different systems** and how different systems may influence each other. Consider the financial sector for example. It plays a critical role for our society and economy. At the same time, the financial system is heavily dependent on digital technology. If a critical digital technological system is disrupted, it may have a major impact on the financial system, with severe knock-on effects on our societal and economic systems.

Recognising the relevance of digital technology for our societal and economic systems, the EU has released **multiple directives and regulations to improve digital resilience**. This includes the new Network and Information Security Directive (NIS2), which is focused on critical infrastructure (such as energy, transport, health and water) (European Parliament & Council of the European Union, 2022a), the Digital Operational Resilience Act (DORA) for the financial sector (European Parliament & Council of the European Union, 2022b), as well as the Cyber Resilience Act (CRA) for products with digital components sold in the EU (European Parliament & Council of the European Union, 2024). In the Netherlands, specifically for the public sector, there is also the Baseline Informatiebeveiliging Overheid (BIO) (Digitale Overheid, z.d.), which is currently undergoing an update, along with the (delayed) implementation of the NIS2 (Rijksoverheid, 2024).

Although on paper these legislative efforts define strong measures to improve digital resilience, **in practice it is often hard to achieve**, especially at a strategic level. A key example in this regard is the reduction of dependency risk from digital technology service providers. DORA, under Article 28(8), for example requires financial sector entities to "put in place exit strategies" for critical Information and communication technology (ICT) service providers, and "identify alternative solutions and develop transition plans enabling them to remove the contracted ICT services and the relevant data from the ICT third-party service provider and to securely and integrally transfer them to alternative providers." The reality however is that often there are no viable alternatives to critical service providers, or that a transition would be too costly.

> "Understanding where and how our digital technology dependencies might impact our societal and economic systems is crucial if we want to make informed choices about the usage of those technologies."

Dutch businesses and organisations are often reliant on non-EU digital technology – and thereby at risk of being at the whims of foreign political agendas (DNB, 2021; ACM, 2022). Digital resilience in the Netherlands and the EU today therefore goes hand-in-hand with **digital sovereignty** – the ability to independently choose and control "the design of and use of (business) critical digital systems" (Stolwijk et al., 2024). Crucially, the Netherlands cannot act in isolation on this front, not least because of its strong social and economic ties with other EU Member States. Collective action and collaboration across the EU are necessary to provide a counterweight to non-EU interests. This was also emphasised by the Dutch state secretary for digitalisation, Zsolt Szabó, in a recent debate, advocating for a European consortium for digital infrastructure, in order to achieve a "more resilient European online ecosystem where privacy, transparency and freedom of choice are central" (Redactie iBestuur, 2025).

While digital sovereignty is not the main focus of this paper, it is important to understand that digital resilience will be more difficult to achieve in a world where we can no longer rely on international partnerships that were taken for granted for decades. Therefore, **digital resilience and digital sovereignty are inexorably linked**. Understanding where and how our non-EU digital technology dependencies might impact our societal and economic systems from a strategic point of view, is crucial if we want to make informed choices about the usage of these technologies – whether that is at a national government level, at the level of individual businesses and organisations, or as citizens (Stolwijk et al., 2024).

To understand the implications of non-EU digital technology dependencies for the resilience of our societal and economic systems, two viewpoints need to be considered: an internal and an external one. The internal viewpoint is about the inherent system risks of our digitally dependent society and economy. The external viewpoint is about the threats posed to the digital resilience of these systems.[4] By combining the two, we can develop an understanding of (1) what the impact is on our society and economy of a disruption of its underlying digital systems, and (2) what scenarios we need to consider that may cause such a disruption. Subsequently, relevant measures can be defined to reduce the risk where needed. Note that **we are not focusing here on temporary disruptions such as short-term unavailability of digital technology, but on strategic/long-term implications for our society and economy.**

4 Note that 'external' here does not necessarily mean threats from abroad (e.g. non-EU threats toward EU systems); rather, it refers to any threats toward the system. In other words, it is about system vs. non-system, not (only) about politics or geography.

3. Case study: challenges in the financial sector

The internal viewpoint – what is the inherent system risk?

Much like utilities such as gas and water, the financial sector is a vital part of the critical infrastructure that sustains our society and economy. However, it is heavily reliant on – predominantly American – service providers such as Visa and Mastercard and technology providers such as Apple and Google (Bassens en Hendrikse, 2022). Encouraged by open banking regulations in the EU, **the financial sector has embraced and incorporated the services and products of 'Big Tech'** (Barbereau et al., 2024). Critically, Big Tech has been resorting to familiar strategies that led to the dominance of Apple in particular: "locking in developers, customers (...) into a hybrid business model based on a synergy between hardware, software and data-driven platform components" (Hendrikse et al., 2018).

Despite the euro being in circulation for over two decades, there are few European infrastructures widely available for both in-store and online transactions. Although the main messaging network through which international payments are initiated (SWIFT) is located in Europe, most existing European payment options are regional in focus and offer only limited functionality. **Non-European payment networks and providers continue to be a key pillar in the value chain**. The market share of American providers Mastercard and Visa is estimated at 61% in Europe (DNB, 2025), and Amazon's cloud solution AWS remains the go-to choice for the backend of gateways and payment processors – largely due to its flexibility and potential to innovate (Barbieri, 2020).

As noted by the European Central Bank, the increasing reliance on foreign providers for payment data storage and processing creates vulnerabilities related to data security, legal jurisdiction, and operational control (ECB, 2024). Becoming more autonomous comes at a cost however as well, namely innovation power and economic competitiveness. The affordances of technological and digital infrastructures provided by Big Tech allow European financial institutions to innovate and be ready for a generation of users native to the Internet. **Strategic coupling between finance and technology is necessary to stay competitive.** The long-term strategic dilemma thus is: how can entities stay in control of their digital resilience while retaining innovation power and economic competitiveness that depend on digital technology that is largely outside of their own control?

> "The strategic dilemma is: how can entities stay in control of their digital resilience while retaining innovation power and economic competitiveness that depend on digital technology that is largely outside of their own control?"

The external viewpoint – what threats do we need to consider?

In today's changing geopolitical landscape, and as part of an escalating transatlantic trade war, **Big Tech and its regulation is used as a bargaining chip** (Rankin, 2025). The current US administration is actively pushing back on digital rules made in Europe – from the Digital Markets Act to the AI Act. In an extreme scenario, we need to consider what happens if the 'plug is pulled' on the payment networks our society and economy rely upon. Naturally, businesses, including Big Tech, have an incentive to maintain and increase their market shares, including in the EU – but that does not mean that they are immune to politics.

A key threat that we need to consider in this context is vendor lock-in. The threat of **vendor lock-in** arises when financial institutions become deeply embedded within proprietary ecosystems – such as cloud platforms, application programming interfaces (APIs), and other products like near field communications (NFCs) used for 'tap and go' payments – controlled by a small number of Big Tech firms. While these systems offer powerful capabilities and operational efficiencies, they often come with high switching costs, limited interoperability, and contractual restrictions that constrain future flexibility (Bassens en Hendrikse, 2022). Over time, this dependency can undermine a firm's ability to adapt its digital strategy, negotiate favourable terms, or align with evolving regulatory needs or other strategic goals. Vendor lock-in is not just a technical issue – it is a strategic vulnerability that can limit innovation, compromise autonomy and expose institutions to external decision-making beyond their control (Prudential Regulation Authority, 2023).

> "Vendor lock-in is not just a technical issue – it is a strategic vulnerability that can limit innovation, compromise autonomy and expose institutions to external decision-making beyond their control."

From a societal perspective, the growing reliance of financial institutions on Big Tech infrastructure can become a threat to European values such as privacy and data protection. As sensitive financial data – often combined with behavioural, biometric, or location information – is processed and stored by third-party platforms, users may lose visibility and control over how their personal information is used, shared or monetised. This raises concerns about profiling, algorithmic decision-making, and the potential for cross-sector data exploitation without informed consent (Doerr et al., 2023). Ultimately, diminished privacy not only erodes trust in digital financial services (which financial institutions predominantly have) (Armantier et al., 2021), but also challenges foundational principles such as digital rights and user agency. Apart from the societal implications, a decrease in trust in a given digital product or service can result in a limited uptake of that product or service and hence a loss of business.

"Diminished privacy not only erodes trust in digital financial services, but also challenges foundational principles such as digital rights and user agency."

To overcome these challenges and solve the strategic dilemma (innovation power and economic competitiveness vs. autonomy and control over the digital resilience of our societal and economic systems), we need to come up with alternative solutions. In other words, **we need to provide businesses and organisations (public and private) with more options to choose from**, e.g. in the form of 'homegrown'/EU-developed digital technology alternatives. Having more choice means having more alternatives – which means being able to adapt to changing circumstances, and thereby becoming more resilient. Of course our resources (financial and talent) are not unlimited, hence we need to prioritise and take a risk-based approach.

"Having more choice means having more alternatives – which means being able to adapt to changing circumstances, and thereby becoming more resilient."

4. Perspective on resilience: a decision-making framework

To increase the scope of action (and choice) on the front of digital resilience and sovereignty, **a tiered approach is required that addresses digital resilience at the various levels of our society and economy**, ranging from the national government to businesses and organisations as well individual users of digital technology. At each level (national, organisational, individual), we need to take stock of what our most important digital assets are, determine to what extent they (should) fall within our scope of control, and subsequently make strategic choices.

While digital sovereignty is essential for digital resilience, it does not mean that we need to be able to do everything ourselves; rather, **we need to focus our efforts on those areas where control is paramount, and let go of other areas where it may be less relevant** – always keeping in mind the strategic dilemma of innovation power and economic competitiveness vs. autonomy and control over the digital resilience of our societal and economic systems. Operating within this tension requires a shift from binary thinking to intentional balancing. In the case of the financial sector for example, rather than choosing between agility and control, or between global platforms and local independence, financial institutions must pursue a hybrid digital strategy – one that ensures competitive capabilities while reducing structural dependencies over time; one that includes several measures and solutions.

Below, a 2-step decision-making framework is provided to support decision-makers. The framework is of general nature, and needs specific tailoring depending on the type of organisation (government, business/organisation, etc.). However, by providing a general outline, we hope to trigger a nuanced approach and thinking toward solving the challenges at hand.

Step 1 – Mapping the landscape

A risk-based approach
A risk-based approach to digital resilience means setting priorities and making choices. From the world of information security, there are relevant frameworks readily available that can help us define such an approach (International Organization for Standardization, 2022a). Typically, it starts with determining the most important assets, followed by a dependency analysis and an assessment of the (desired) level of control. This forms Step 1 of our approach. After an understanding is developed of how sensitive a given digital asset is to our societal and economic systems, we can subsequently make decisions to put relevant safeguards in place; in risk management terms: define risk treatment strategies. This forms Step 2 of our approach.

What are our most important assets?
From a national perspective, as a first proxy, we can start with the sectors defined in the NIS2 (energy, transport, banking, health, water, ICT, finance, public administration, etc.). For each sector, we then need to determine what the **digital 'crown jewels'** are that require utmost protection.[5] We do this for each level of the technological stack (digital infrastructure, data, applications, etc.).

What dependencies do we have?
Once we have established the 'crown jewels', we need to assess to what extent they are dependent on digital service and technology providers outside of our direct control – considering the entire value chain (not only our own suppliers, but also our suppliers' suppliers, etc.). Only by **looking at the entire digital ecosystem** we can come to a full assessment of dependencies.

How much control do we (want to) have over the dependencies?
Once we understand our dependencies within all critical sectors and at all levels of the technological stack, we can start assessing to what extent we have control over them. Even when they may not fall under our direct control, we may still have other means to control them. At a local government level, for example, municipalities may team up to collectively procure digital services, increasing their **bargaining power** over a digital technology provider. There are also situations where, even if an asset is outside of our own direct control, we may – from a risk-based perspective – decide that we are perfectly fine with that situation. This would be the case if control is exercised by a reliable partner, for example.

5 A classic method that can be used to categorise the criticality of a digital asset is the so-called CIA triad – referring to the (desired) Confidentiality, Integrity, and Availability of the assessed asset.

Step 2 – Making strategic choices

Strategic options
For each critical digital asset, once we have established to what extent it falls within our (desired) control, we can apply different strategies to bring the current level of control to our desired level. Multiple strategies can be applied, depending on the outcome of the analysis.

Reducing digital dependency
To reduce an undesirable digital dependency, a practical solution is to define alternative ways of working that allow for a minimum level of operations under adverse circumstances for a defined period of time – we can think of this as the 'survival mode'. This strategy stems from the world of **business continuity and crisis management**, and there are multiple existing frameworks in place that can help (International Organization for Standardization, 2019 & 2022b). In essence, it means switching from a digital to a manual way of working. While this may not be a viable solution for all digital technologies, it can be for some and should therefore be considered as a possible strategy.

Develop or procure own/alternative solutions
If reducing digital dependency is not a viable option, another strategy is to develop (or procure) own/alternative digital technology solutions to the currently available ones. However, for critical digital technology assets this may often not be possible. Therefore this strategy requires a longer-term vision and **public-private collaboration**, where government entities help to facilitate innovation through investments or by serving as a launching customer for a new technology. The Netherlands, for example, is actively identifying and investing in digital technologies where national (or at least EU) control is foreseen as strategically relevant in the near future (specifically in the areas AI, data, cloud and cyber) (Rijksoverheid, 2025).

Increase bargaining power
If neither a reduction of nor alternative to a digital dependency are feasible, **building alliances** with partners to increase bargaining power is a viable alternative option. This option is particularly interesting from a digital ecosystem perspective. Where multiple entities (public and/or private) depend on a critical digital technology, collective action can strengthen the position and leverage over a provider. This can be a relevant strategy also for digital technology dependencies that are not at the national security level, but may still have a major impact on the resilience of our society and economy.

Exercise control via other means
A fourth option can be to exercise control via other means. This is typically a strategy that can be applied from a national level as part of **foreign policy**, less so by individual entities or sectors. While the use of force may be the most extreme 'other mean' to exercise pressure, lower-level measures in the form of 'soft power' should be considered (Nye, 2017). Another useful approach in this regard can be to establish control points (Pisa et al., 2024), thereby creating a dependency for another party in one area, which in turn can be used to balance the dependency we have from that party in another area.

Accept the risk
Should all strategies to manage a dependency be exhausted, the only remaining option is to accept the risk. While this may not be desirable, at least it helps to provide visibility on where the 'pain points' are of our societal and economic systems from a digital resilience perspective. Having **clarity on your risk landscape** is better than operating under high levels of uncertainty.

5. Conclusion

"Dependency comes at a price, but so does autonomy. Finding the balance within the strategic dilemma is a challenge that will always be evolving and require us to evolve with it."

Making **informed strategic choices** about the usage of digital technologies that our societal and economic systems depend upon, is necessary to strengthen resilience. By performing a risk-based assessment at the various levels of our society and economy (national/government, businesses/organisations, and individual users/citizens) – across the entire digital technology stack (digital infrastructure, data, applications, etc.) – we can develop a nuanced approach to counter the challenges and seize the opportunities of today's highly dynamic, political landscape.

Collaboration is essential, not only between private and public parties, but across borders, especially within the EU. We cannot act in isolation, but need to share resources and strengthen our bargaining power by acting collectively. Digital resilience requires an **ecosystem approach**:

- The national government, its ministries, must play a role in broadening the scope of choice in terms of digital technology for businesses and organisations (public and private) – through investments, facilitating innovation and spearheading the application of 'homegrown' digital technology where this is relevant for digital resilience.
- Businesses and organisations (public and private), need to evaluate – from a societal and economic perspective – where they are vulnerable to external threats in terms of their digital dependencies and take appropriate, strategic action.
- Individual users of digital technology should (be enabled to) make informed decisions about which technologies they want to rely upon, which businesses they want to share their data with, and how their user behaviour links to the digital resilience of our society and economy.

Each element of the ecosystem matters for its overall resilience**; each choice has implications for the entire system**. Our society and economy will always be embedded in an international playing field, with conflicting interests, power dynamics, and values. Dependency comes at a price, but so does autonomy. Finding the balance within the strategic dilemma of innovation power and economic competitiveness vs. autonomy and control over the digital resilience of our societal and economic systems, is a challenge that will always be evolving. It requires us to adjust and evolve with it.

References

Armantier, O., Doerr, S., Frost, J., Fuster, A., & Shue, K. (2021). *Whom do consumers trust with their data? US survey evidence* (BIS Bulletin No. 42). 27 May 2021. Bank for International Settlements. https://www.bis.org/publ/bisbull42.pdf

Autoriteit Consument & Markt (ACM) (2022). *Market study cloud services.* 5 september 2022. https://www.acm.nl/system/files/documents/public-market-study-cloud-services.pdf

Barbereau, T., Weigl, L., & Pocher, N. (2024). Financial regulation, political context, and technology in the European Union. In G. Fridgen et al. (Eds.), *Decentralization technologies: Financial sector in change* (pp. 19–46). Springer. https://doi.org/10.1007/978-3-031-66047-4_2

Barbieri, V. (2020). *The use of cloud computing by financial institutions.* Cloud Banking Forum, European Banking Federation. https://www.ebf.eu/wp-content/uploads/2020/06/EBF-Cloud-Banking-Forum_The-use-of-cloud-computing-by-financial-institutions.pdf

Bassens, D., & Hendrikse, R. (2022). Asserting Europe's technological sovereignty amid American platform finance: Countering financial sector dependence on Big Tech? *Political Geography, 97*, 102648. https://doi.org/10.1016/j.polgeo.2022.102648

Damen, M. (2022). *EU strategic autonomy 2013–2023: From concept to capacity* (Briefing No. 733.589). European Parliamentary Research Service, Strategic Foresight and Capabilities Unit. https://www.europarl.europa.eu/thinktank/en/document/EPRS_BRI(2022)733589.

De Nederlandsche Bank (DNB) (2021). *Changing landscape, changing supervision: Developments in the relationship between BigTechs and financial institutions.* https://www.dnb.nl/media/32apiuom/dnb-big-tech-supervision-changing-landscape-changing-supervision.pdf

De Nederlandsche Bank (DNB) (2025). *DNB jaarverslag 2024: Robuust beleid in een onzekere wereld.* https://www.dnb.nl/media/mtyf3rtu/dnb-jaarverslag-2024.pdf

Digitale Overheid (z.d.). *Baseline Informatiebeveiliging Overheid.* Geraadpleegd op 7 mei 2025, https://www.digitaleoverheid.nl/overzicht-van-alle-onderwerpen/cybersecurity/bio-en-ensia/baseline-informatiebeveiliging-overheid/

Doerr, S., Gambacorta, L., Guiso, L., & Sanchez del Villar, M. (2023). *Privacy regulation and fintech lending* (BIS Working Papers No. 1103). Bank for International Settlements. https://www.bis.org/publ/work1103.htm

Duke, S. (2025). *AI is changing work – The time is now for strategic upskilling.* World Economic Forum. https://www.weforum.org/stories/2025/04/linkedin-strategic-upskilling-ai-workplace-changes/

European Central Bank (ECB) (2024). *ECB guide on outsourcing cloud services to cloud service providers* (Draft Guide). https://www.bankingsupervision.europa.eu/framework/legal-framework/public-consultations/pdf/ssm.pubcon240603_draftguide.en.pdf

European Commission (2020). *Communication from the Commission to the European Parliament and the Council: 2020 strategic foresight report – Strategic foresight: Charting the course towards a more resilient Europe* (COM(2020) 493 final). https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52020DC0493

European Parliament & Council of the European Union (2022a). *Directive (EU) 2022/2555 of the European Parliament and of the Council on measures for a high common level of cybersecurity across the Union, amending Regulation (EU) No 910/2014 and Directive (EU) 2018/1972, and repealing Directive (EU) 2016/1148 (NIS 2 Directive).* http://data.europa.eu/eli/reg/2024/1689/oj/eng

European Parliament & Council of the European Union (2022b). *Regulation (EU) 2022/2554 of the European Parliament and of the Council on digital operational resilience for the financial sector and amending Regulations (EC) No 1060/2009, (EU) No 648/2012, (EU) No 600/2014, (EU) No 909/2014 and (EU) 2016/1011 (Digital Operational Resilience Act). Official Journal of the European Union,* L 333, 1–79. https://eur-lex.europa.eu/eli/reg/2022/2554/oj/eng

European Parliament & Council of the European Union (2024). *Regulation (EU) 2024/2847 of the European Parliament and of the Council on horizontal cybersecurity requirements for products with digital elements and amending Regulations (EU) No 168/2013 and (EU) 2019/1020 and Directive (EU) 2020/1828 (Cyber Resilience Act). Official Journal of the European Union,* L 2024/2847. https://eur-lex.europa.eu/eli/reg/2024/2847/oj/eng

Hendrikse, R., Bassens, D., & van Meeteren, M. (2018). The Appleization of finance: Charting incumbent finance's embrace of FinTech. *Finance and Society,* 4(2), 159–180. https://doi.org/10.2218/finsoc.v4i2.2870

Henley, J., Kassam, A., & Jones, S. (2025). *Tens of Millions across Spain and Portugal Hit by Huge Power Outage.* 28 April 2025, The Guardian. https://www.theguardian.com/world/2025/apr/28/spain-portugal-power-outage.

International Organization for Standardization (2019). *ISO 22301:2019 – Security and resilience – Business continuity management systems – Requirements.* https://www.iso.org/standard/75106.html

International Organization for Standardization (2022a). *ISO/IEC 27005:2022 – Information security, cybersecurity and privacy protection: Guidance on managing information security risks* (4th ed.). https://www.iso.org/standard/80585.html

International Organization for Standardization (2022b). *ISO 22361:2022 – Security and resilience – Crisis management – Guidelines.* https://www.iso.org/standard/50267.html

Nye, J. S. (2017). Soft power: The origins and political progress of a concept. *Palgrave Communications, 3*(1), 1–3. https://doi.org/10.1057/palcomms.2017.8

Pisa, D., van der Mark, M., & van der Meulen, M. (2024). *Grip op control points: Gerichter innoveren.* TNO. https://vector.tno.nl/artikelen/grip-control-points-gerichter-innoveren/

Prudential Regulation Authority (2023). *Outsourcing and third party risk management* (Supervisory Statement SS2/21). Bank of England. https://www.bankofengland.co.uk/paper/2023/ss/outsourcing-third-party-risk-management-ss-recognised-payment-system-operators

Rankin, J. (2025). *EU will not rip up tech rules for trade deal with Trump, senior official says.* 11 April 2025. The Guardian. https://www.theguardian.com/world/2025/apr/11/eu-will-not-rip-up-tech-rules-for-trade-deal-with-trump-senior-official-says

Redactie iBestuur (2025). Nederland in EU-consortium voor digitale infrastructuur. 17 januari 2025. iBestuur (Nieuwseditie). https://ibestuur.nl/artikel/nederland-in-eu-consortium-voor-digitale-infrastructuur/

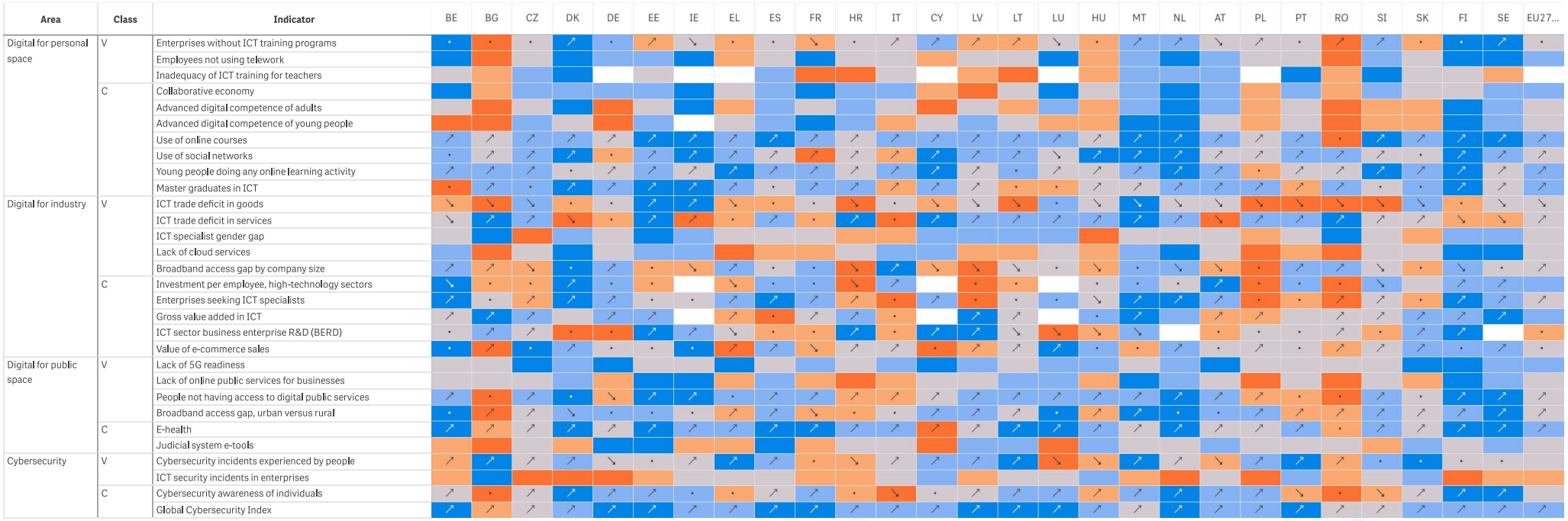
Rijksoverheid (2024). *Implementatie NIS2 en CER in Nederland vertraagd, wat betekent dat voor u?* https://www.rijksoverheid.nl/actueel/nieuws/2024/10/23/implementatie-nis2-en-cer-in-nederland-vertraagd-wat-betekent-dat-voor-u

Rijksoverheid (2025). *Nederland trekt financiering voor AI, data, cloud en cybersecurity innovatie aan.* 29 april 2025. https://www.rijksoverheid.nl/actueel/nieuws/2025/04/29/nederland-trekt-financiering-voor-ai-data-cloud-en-cybersecurity-innovatie-aan

Ross, R., Pillitteri, V., Graubart, R., Bodeau, D., & McQuaid, R. (2021). *Developing cyber-resilient systems: A systems security engineering approach* (NIST Special Publication 800-160, Vol. 2, Rev. 1). National Institute of Standards and Technology. https://www.nist.gov/publications/developing-cyber-resilient-systems-systems-security-engineering-approach-0

Stolwijk, C., van der Meulen, M., Pisa, D., & van der Mark, M. (2024). *Towards a sovereign digital future – The Netherlands in Europe* (p. 5). TNO. https://vector.tno.nl/en/articles/digital-transformation-europe/

Annex I – EU Digital Resilience Dashboard



Area	Class	Indicator	BE	BG	CZ	DK	DE	EE	IE	EL	ES	FR	HR	IT	CY	LV	LT	LU	HU	MT	NL	AT	PL	PT	RO	SI	SK	FI	SE	EU27...
Digital for personal space	V	Enterprises without ICT training programs	•	•	•	↗	•	↗	↘	•	•	↘	•	↗	↗	↗	↗	↘	•	↗	↗	↘	↗	•	↗	↗	•	•	↗	•
		Employees not using telework																												
		Inadequacy of ICT training for teachers																												
	C	Collaborative economy																												
		Advanced digital competence of adults																												
		Advanced digital competence of young people																												
		Use of online courses	↗	↗	↗	↗	↗	↗	↗	↗	↗	↗	↗	↗	↗	↗	↗	↗	↗	↗	↗	↗	↗	↗	•	↗	↗	↗	↗	↗
		Use of social networks	•	↗	↗	↗	•	↗	↗	↗	↗	↗	↗	↗	↗	↗	↗	↘	↗	↗	↗	↗	↗	↗	↗	↗	•	↗	↗	↗
		Young people doing any online learning activity	↗	↗	↗	•	↗	↗	↗	↗	↗	↗	↗	↗	↗	↗	•	↗	↗	↗	↗	↗	•	↗	↗	↗	↗	↗	↗	↗
		Master graduates in ICT	•	↗	•	↗	↗	↗	↗	↗	•	↗	↗	↗	↗	↗	•	•	↗	↗	↗	↗	↗	↗	↗	•	•	↗	↗	↗
Digital for industry	V	ICT trade deficit in goods	↘	↘	↘	•	•	↗	↗	↘	•	•	↘	•	↘	↘	↘	•	↘	↘	↘	↘	↘	↘	↘	↘	↘	•	↘	↘
		ICT trade deficit in services	↘	↗	↗	↘	•	↗	↗	•	↗	•	↗	•	↗	↗	↗	↗	↗	↗	↗	↘	↗	↗	↗	↗	↗	↘	↘	↗
		ICT specialist gender gap																												
		Lack of cloud services																												
		Broadband access gap by company size	↗	↗	↘	•	↗	•	↘	↗	•	•	↘	↗	↘	↘	↘	•	↘	•	↘	↘	•	↗	↗	↘	•	↘	•	↗
	C	Investment per employee, high-technology sectors	↘	•	•	↗	•	•		↘	•	•	↘	↗		•	•		•	•	•	↗	•	•	•	↘		↗	↗	
		Enterprises seeking ICT specialists	↗	•	↗	↗	↗	•	•	↗	↗	↗	↗	•	↗	•	•	•	↘	↗	↗	↗	•	•	↗	↗	•	↗	↗	↗
		Gross value added in ICT	↗	↗	↗		↗	↗		↗	•	↗	↗	•		↗	↗		•	↗		↗	↗		↗	↗	↗	↗	↗	
		ICT sector business enterprise R&D (BERD)	•	↗	↗	•	•	↗	↗	↘	•	•	↗	•	↗	↗	↘	↘	↘	↘		•	•	•	↗	•	↗	↗		•
		Value of e-commerce sales	•	↗	•	↗	•	•	•	↗	↗	↘	↗	↗	•	↗	↗	↗	•	•	↗	•	↗	•	↗	↗	↗	•	↗	•
Digital for public space	V	Lack of 5G readiness																												
		Lack of online public services for businesses																												
		People not having access to digital public services	↗	•	↗	•	↘	↗	↗	•	↗	↗	↗	↗	↗	↗	↗	↗	↗	↗	↗	↗	↗	•	•	↗	•	↗	↗	↗
		Broadband access gap, urban versus rural	•	↗	↗	↘	•	•	•	↗	↗	↘	•	•	↗	↗	↗	•	↗	↗	•	•	↗	↗	↗	↗	↗	↗	↗	↗
	C	E-health	↗	↗	↗	↗	↗	↗	↗	↗	↗	↗	↗	↗	↗	↗	↗	↗	↗	↗	↗	↗	↗	↗	•	↗	↗	↗	↗	↗
		Judicial system e-tools																												
Cybersecurity	V	Cybersecurity incidents experienced by people	↗	↗	↗	↗	↘	•	↗	↗	↗	•	↘	↗	↗	↗	↗	↘	↘	↗	↗	↘	↗	↗	↗	•	•	•	•	
		ICT security incidents in enterprises																												
	C	Cybersecurity awareness of individuals	↗	•	↗	↗	↗	↗	•	•	↗	↗	•	↘	•	↗	↗	↗	↗	↗	↗	↗	↗	↗	↘	•	↘	↗	↗	↗
		Global Cybersecurity Index	↗	↗	↗	↗	↗	↗	↗	↗	↗	↗	↗	↗	↗	↗	↗	↗	↗	↗	↗	↗	↗	↗	↗	↗	↗	↗	↗	↗

C = Capacities, V = Vulnerabilities

Data typically refers to 2018-2022. The colours indicate the position of a country in the distribution of all available values for EU countries in the 2015-2022 reference period. An upward pointing arrow for a vulnerability indicates a substantial reduction (improvement). The change in time has been removed for LFS based series with systematic breaks in the original data series for 2021 (Employees not using telework and ICT specialist gender gap).

Resilience

- Highest capacities / Lowest vulnerabilities
- Medium-high capacities / Medium-low vulnerabilities
- Medium capacities/vulnerabilities
- Medium-low capacities / Medium-high vulnerabilities
- Lowest capacities / Highest vulnerabilities
- Not available

Change with regards to 2017

- ↗ Sizable improvement
- • Not sizable
- ↘ Sizable worsening
- A plain cell marks not enough data to compute the arrow

Source: https://commission.europa.eu/strategy-and-policy/strategic-foresight/2020-strategic-foresight-report/resilience-dashboards_en (5 May 2025)

Authors
Augustinus Mohn & Tom Barbereau

With acknowledgements to: Anastasia Yagafarova, Gerben Broenink, Anne Fleur van Veenstra & Alexander van den Wall Bake

June 12 2025

TNO Vector
Centre for Societal Innovation and Strategy

tnovector.nl