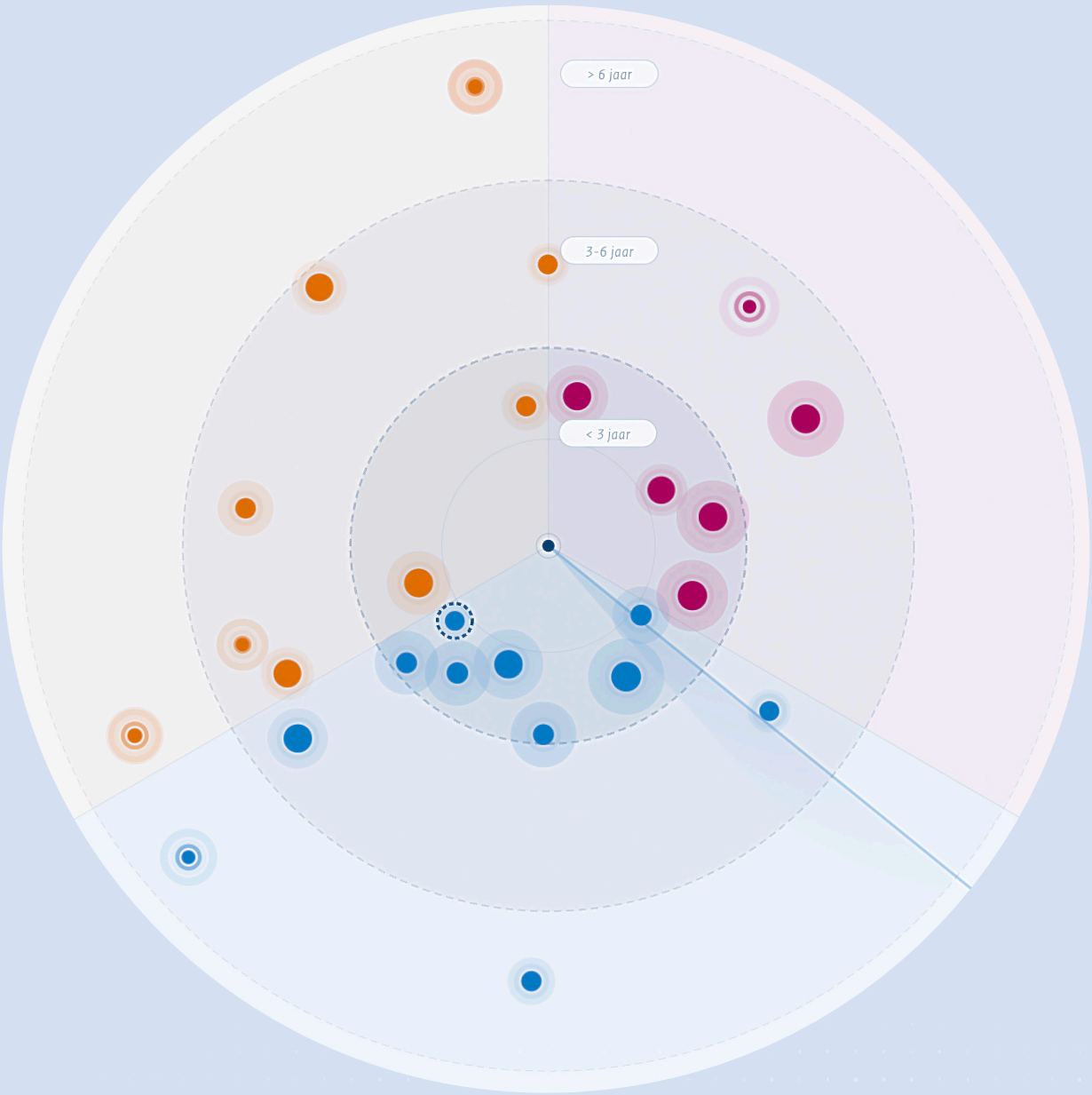
Dutch Authority for Digital Infrastructure
Ministry of Economic Affairs and Climate Policy



Trend Radar 2026 - 2035

Dutch Authority for Digital Infrastructure
For a **securely connected** Netherlands

Inhoud

Tomorrow's digital infrastructure on today's radar 3

Technological developments 4

Growing demand for radio spectrum driving scarcity and vulnerability 5

Agentic AI taking the reins 6

The three dimensional evolution of networks 7

Quantum technology placing new demands on digital resilience 8

Emergence of sensing technology 9

AI taking on a physical form 10

AI accelerating scientific practice 11

Photonic chips 12

DNA-based data storage shows great promise; currently out of reach 13

Geopolitical developments 14

Digital infrastructure as a geopolitical lever 15

Cyberattacks becoming more covert and less direct 16

AI increasingly used for cyberattacks and cyber defence 17

Digital autonomy high on the political agenda 18

Growing focus on strategic autonomy in raw materials and semi-finished products 19

Foreign interference undermining earning capacity in the Netherlands 20

Societal developments 21

Legislation in a bind between risk management and digital innovation 22

Digital infrastructure interwoven into every aspect of our lives 23

Synthetic identities increasing pressure on digital trust frameworks 24

Growing demand for energy and water 25

Influx of non-compliant equipment increasing safety risks 26

The digital resilience gap between SMEs and large enterprises 27

The vicious cycle of AI and disinformation 28

Availability of digital infrastructure under pressure 29

Shortage of professionals straining availability and innovation 30

Weather extremes increasing vulnerability of digital infrastructure 31

New human machine interfaces 32

Conclusion 33

References 34

Tomorrow's digital infrastructure on today's radar

Available, reliable and continuously operational digital infrastructure is essential to the functioning of our society. That is a hard fact, even though the digital infrastructure itself is anything but fixed. Technological breakthroughs, societal shifts and geopolitical tensions drive constant change, making infrastructure more complex and increasingly vulnerable.

Using the Trend Radar, the Dutch Authority for Digital Infrastructure (RDI) identifies and analyses developments that will affect our digital infrastructure over the next ten years. RDI uses the radar as a tool to prioritise regulatory activities, anticipate developments in good time and take action where necessary. This report also supports policymakers, businesses and other professionals in the digital infrastructure sector in managing risks and capitalising on opportunities.

Our colleagues worked with 30 experts from the business sector, research organisations and government bodies to identify the 26 most important trends, from breakthroughs in quantum technology and AI to the growing pressure on energy supplies and the effects of extreme weather. The trends reveal the broad range of societal challenges facing both RDI and society as a whole.
The trends are divided into three themes: technology, geopolitics and society. Each trend on the radar is given a score (high, medium or low) indicating its expected impact on the digital infrastructure. The radar also indicates the timeframe within which the trend is expected to peak.

We invite you to explore these trends and join us in considering what they mean for the digital infrastructure of tomorrow. After all, identifying emerging developments is only the first step—turning them into policy, investment and cooperation is up to all of us.

What do the impact scores mean?

high Major effect on the digital infrastructure, often on the system as a whole. Consequences felt by a large share of society.

medium Medium effect on the digital infrastructure or parts thereof. Consequences felt by a medium share of society.

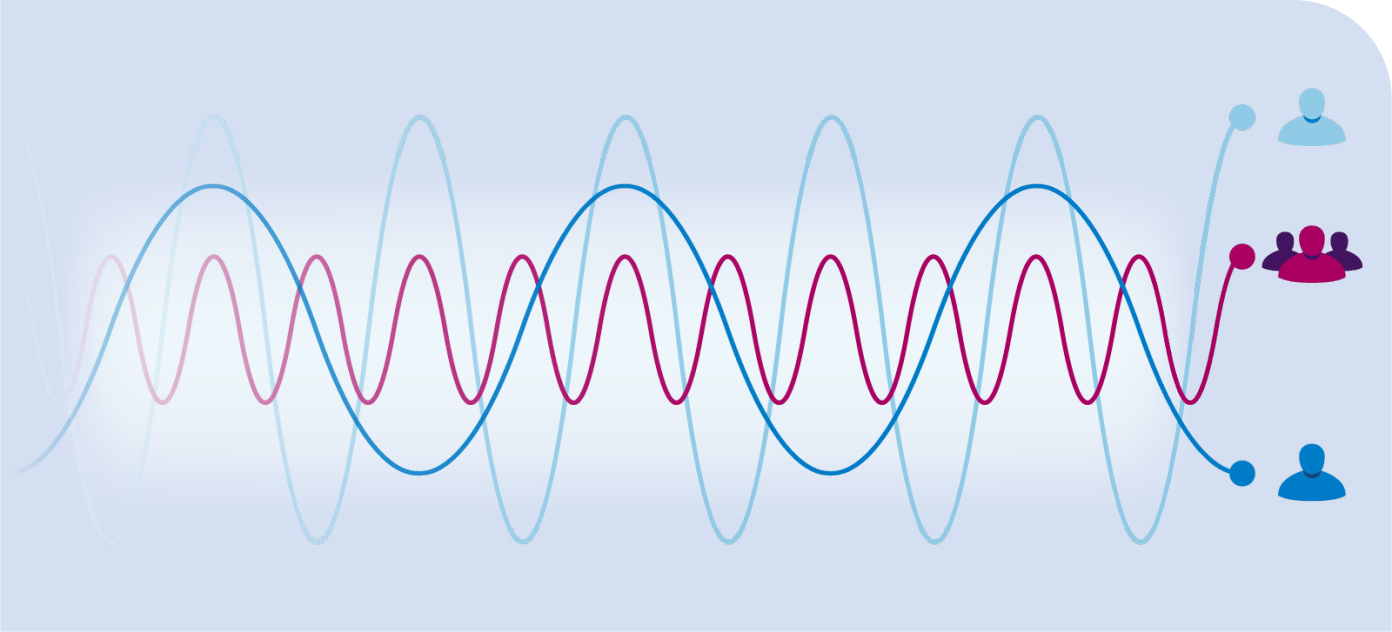
low Limited effect on the digital infrastructure or small parts thereof. Consequences felt by a small share of society.

Technological developments

Technological breakthroughs are emerging in rapid succession and have a high and direct impact on the digital infrastructure and the sectors dependent on it. They open up new possibilities but also introduce new risks. Developments now appearing on the radar include key Technologys such as various forms of AI and quantum technology, as well as changes in satellite technology, have a high impact on the digital infrastructure.

Growing demand for radio spectrum driving scarcity and vulnerability

Impact **high** Timeframe **< 3 years**



The growing demand for radio spectrum is creating scarcity in specific frequency bands. This development is driven in part by the rapidly increasing need for more spectrum in higher bands (Q/V/E and above) for satellite applications.

Joint use of frequencies ('spectrum sharing') helps ease this scarcity. Interest in spectrum sharing is growing steadily. Technologies that enable spectrum sharing on a larger scale are advancing rapidly. One such technology is 'cognitive radio', which enables devices to coordinate among themselves and with the network to select the appropriate frequency and transmission power.

Impact

Increasing strain on the radio spectrum can lead to interference in licence exempt bands, where the use of applications such as satellite communications, Wi Fi, Bluetooth and Long Range (LoRa) devices is becoming more widespread. Such interference poses particular risks for critical applications, including medical equipment. Increasing congestion also affects radio astronomy, as the bands it observes are increasingly being used for terrestrial applications.

More efficient use of the spectrum through developments such as cognitive radio increases the efficiency of spectrum utilisation, but also requires new regulations. Licences often still assume that usage rights for a specific part of the spectrum are assigned to a specific user, whereas cognitive radio must be able to coordinate among multiple users across a larger portion of the spectrum. The high level of complexity involved in cognitive radio also makes it more prone to failure.

In addition, like the broader digital infrastructure, the radio spectrum is increasingly becoming a geopolitical and strategic domain. Hybrid threats such as deliberate jamming, spoofing and the use of drones have an even greater impact due to spectrum congestion. The impact is especially significant for applications that require reliable radio communications, such as GPS/GNSS, emergency services (C2000/P2000), the medical sector, defence and aviation.

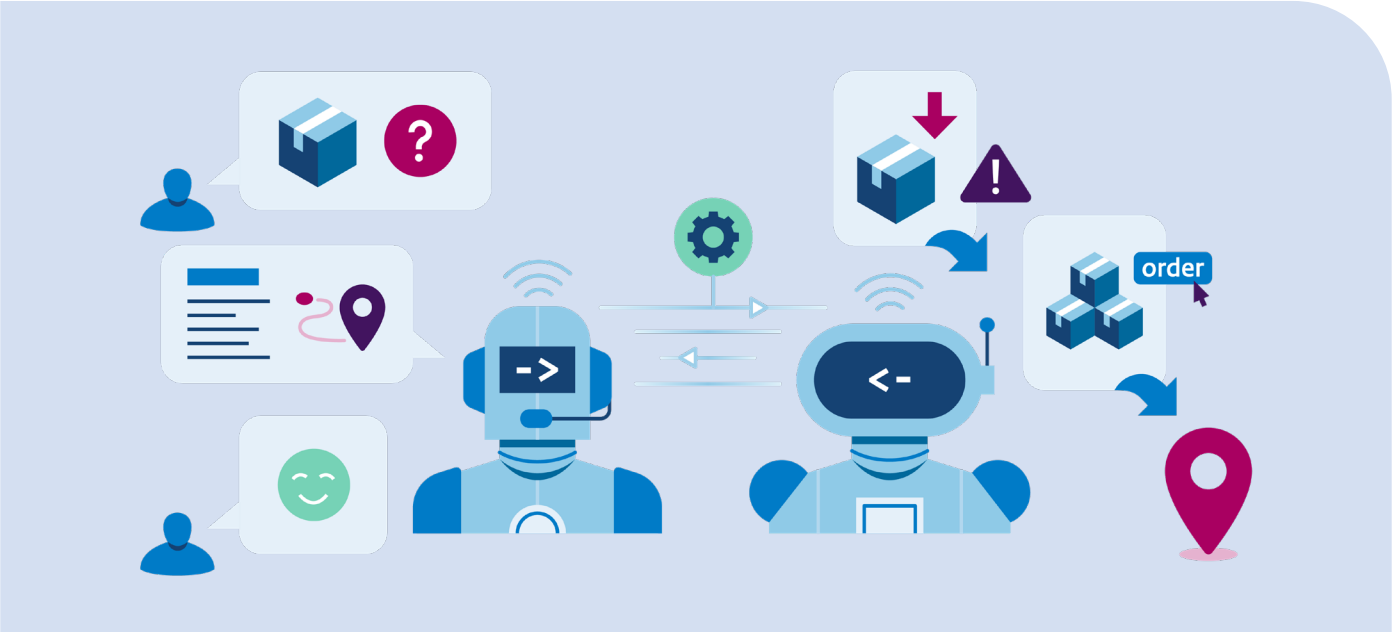
See also

22 Legislation in a bind between risk management and digital innovation

29 Availability of digital infrastructure under pressure

Agentic AI taking the reins

Impact **high** Timeframe **0–3 years**



AI models are capable of processing and analysing vast amounts of information at high speed, ranging from video footage and audio recordings to research reports and unstructured data sources. Since 2025, various AI systems have increasingly been linked together and assigned a goal that is achieved largely autonomously. This is known as agentic AI,

and it has a wide range of potential applications. For example, an autonomous digital assistant can independently decide to order groceries based on previous conversations, calendar information and the amount of food in stock. However, agentic AI can also be used to carry out sophisticated, autonomous ransomware attacks or to independently identify and exploit security vulnerabilities. With the increasing number of linked data sources (e.g., consumer and traffic cameras, smart devices, administrative systems and health monitoring tools) agents can tap into ever larger pools of unstructured information they can combine and use to support decision making.

Because these systems learn from new data and previous results, their analyses, decisions and autonomous actions are becoming increasingly sophisticated, accurate and targeted.

Impact

Provided they have the necessary authorisation and authentication, autonomous agents can independently conduct transactions, control systems and make decisions on behalf of users. This fundamentally shifts the role of AI: AI no longer merely supports decision making but can also independently manage digital and physical processes to achieve predefined objectives.

See also

11 AI accelerating scientific practice

16 Cyberattacks becoming more covert and less direct

17 AI increasingly used for cyberattacks and cyber defence

The three dimensional evolution of networks

Impact **high** Timeframe **3–6 years**



Improvements in satellite technology are enabling three-dimensional networks, which extend not only two-dimensionally across the surface but also vertically, in height. Such networks can include many types of satellites, from Low Earth Orbit (LEO) and geostationary satellites to 'High Altitude Platform Systems' (HAPS) like drones and balloons. Satellites also increasingly communicate directly with users' devices ('Direct-to-Device', D2D), instead of serving as a link in the network infrastructure.

Impact

Due to redundancy in connection types and capacity, 3D networks offer higher availability and better coverage. Improved availability comes from the system's ability to automatically fall back on whichever technology is still working when coverage drops or a connection fails. The system also allows for dynamic capacity allocation: when demand surges, such as at a large event or in an emergency zone, HAPS or satellite beams can deliver extra capacity to specific coordinates.

3D networks are also suitable for areas with limited coverage, such as for autonomous agricultural vehicles, maritime logistics and environmental monitoring. The impact of these applications is likely to be limited in the European part of the Netherlands, as good mobile coverage is already available through existing networks. The benefits are more significant in the Caribbean Netherlands.

The standardisation and assurance of interoperability in 3D networks are important first steps. Interoperability will make connections independent of the underlying network, allowing customers to take out connectivity contracts without choosing a specific medium such as cable, fibre, mobile or satellite.

3D networks raise new questions for governments regarding regulation. Space legislation is complex, and existing regulations often focus on individual technologies, while 3D networks combine multiple connection types. This raises new questions regarding the responsibilities and obligations of network operators, such as resolving faults in 3D networks and lawful interception obligations. Space is also becoming increasingly crowded due to the growing number of satellites, increasing the risk of collisions and space debris.

The move toward three dimensional networking may allow new providers to enter the market. At the same time, there is a risk that merging networks will result in fewer providers and a concentration of power. Europe recognises this risk and is investing in a European satellite constellation in the form of IRIS2.

See also

5 Growing demand for radio spectrum driving scarcity and vulnerability

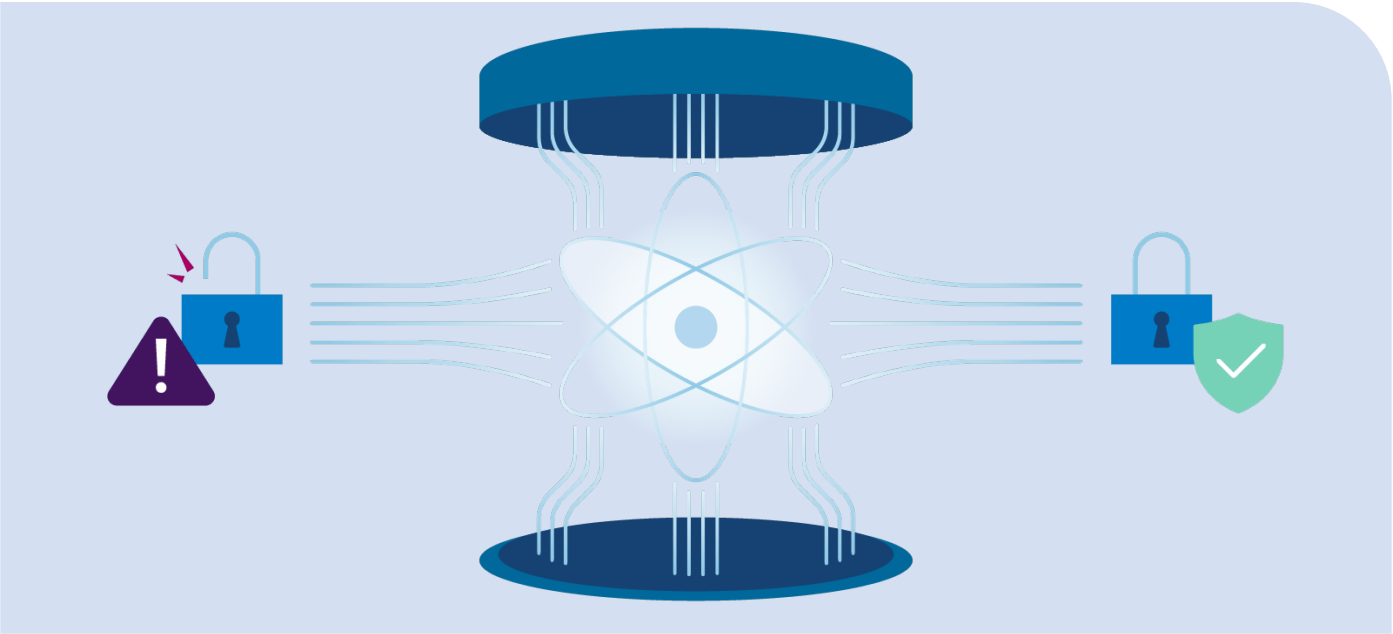
22 Legislation in a bind between risk management and digital innovation

23 Digital infrastructure interwoven into every aspect of our lives

29 Availability of digital infrastructure under pressure

Quantum technology placing new demands on digital resilience

Impact **high** Timeframe **3–6 years**



Quantum computers have the potential to fundamentally change the security of digital systems. There are quantum algorithms that would allow a sufficiently powerful quantum computer to break many current forms of encryption, making confidential information readable. Fully-fledged quantum computers will likely not exist for several more years, yet they already pose a real threat. State actors can store encrypted communications today in the expectation that they will be able to decrypt them later ('harvest now, decrypt later').
As such, quantum technology is considered a strategic weapon.
Two solutions are being developed: post quantum cryptography (PQC) and quantum key distribution (QKD).
QKD is a technique for generating and exchanging keys securely. The exchanged key is then used for traditional encryption that cannot be broken by quantum computers, or for post quantum cryptography. PQC consists of new forms of encryption that—based on current knowledge—cannot be broken by quantum computers.
QKD requires quantum networks that can transmit quantum information instead of digital information. This is still a major challenge, particularly over long distances.
In the long term, access to quantum computers is likely to become easier as they become available as a cloud service.

Impact

Without intervention, all our confidential financial, medical and commercially sensitive information will be accessible to malicious, potentially state-backed, actors within a few years. It is therefore essential that organisations begin the transition to quantum-safe security now, even in the absence of a legal obligation.
Switching from traditional encryption to PQC requires attention and time.
Not all organisations are sufficiently aware of the need and the urgency. In addition, the transition may require new hardware or protocols. Many sectors use assets with long service lives that cannot be upgraded to PQC through software updates during their operational lifetime.
The societal impact is determined by tech companies and their design choices, not by the wishes or expectations of users and society. Large tech companies can become 'gatekeepers'— not only because they control the hardware, but also because they control the software, which is an essential component for using quantum technology.
This impact is less visible than that of the first generation of quantum technology, which consisted of semiconductors, chips and lasers. Fallback options and traditional alternatives to digital communication (e.g., courier services) are disappearing, while digital and quantum threats are on the rise.

See also

16 Cyberattacks becoming more covert and less direct

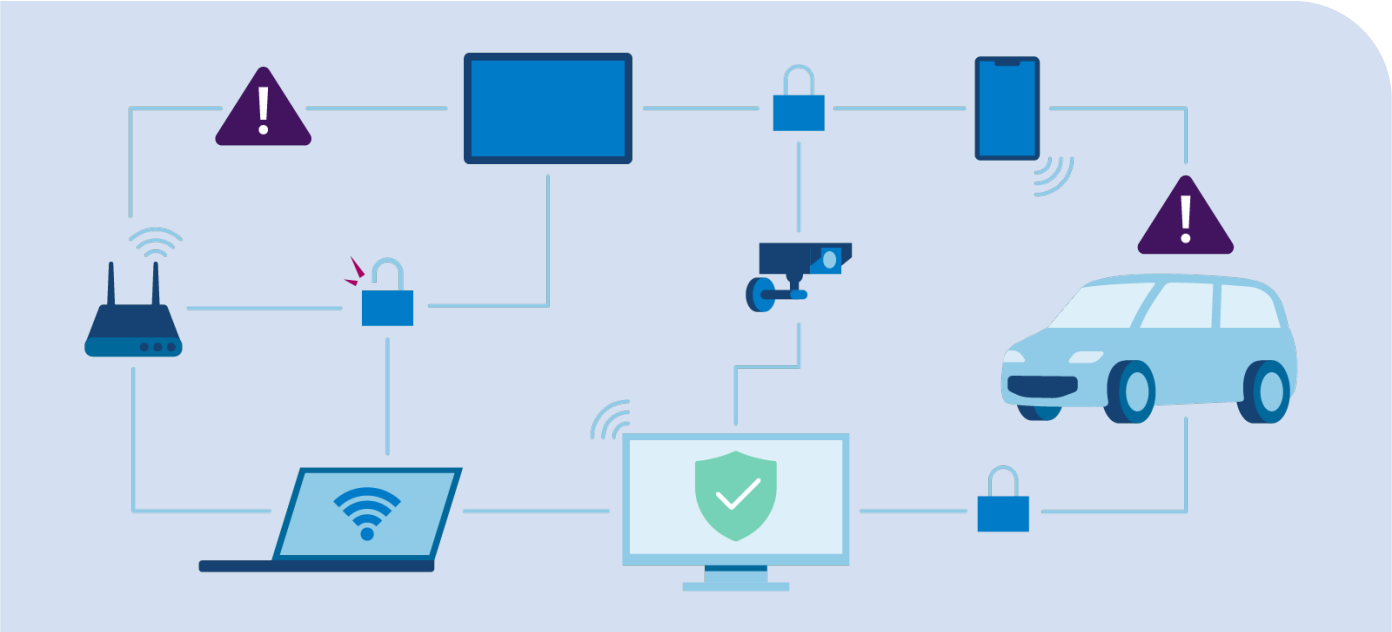
18 Digital autonomy high on the political agenda

19 Growing focus on strategic autonomy in raw materials and semi-finished products

27 The digital resilience gap between SMEs and large enterprises

Emergence of sensing technology

Impact **medium** Timeframe **3–6 years**



In sensing technology, systems use multiple types of sensors, combining the collected sensor data and analysing it in context, often using artificial intelligence (AI). This results in new applications in which systems perceive, understand and respond to their environment with increasing accuracy. Two key developments in sensing technology are Integrated Sensing and Communication (ISAC) in 6G mobile networks and the emergence of quantum sensors.
ISAC combines communication and sensing using the radio waves from 5G and 6G antennas for both data transmission and detection and measurement. For example, at a junction, the system can detect the presence, position and movement of people and vehicles, using that information to improve traffic safety.

Quantum sensors enable extremely accurate measurements by utilising quantum mechanical properties. One promising breakthrough is the development of new quantum sensors that enable accurate positioning without relying on GNSS systems. Quantum sensors' capabilities are generally enhanced further when they are interconnected via a quantum network instead of via traditional digital networks.

Impact

A positive development for the digital infrastructure is that sensing enables the detection of vulnerabilities, faults and performance issues at an early stage. This allows network operators to improve the continuity and availability of digital infrastructure. The technology also offers new opportunities for other sectors. In industrial environments, the development of sensing technology supports the emergence of autonomous production lines, and sensors (including quantum sensors) support applications such as preventive maintenance. Personnel safety can also be improved, e.g., through automatic fall detection systems for maintenance workers.
The downside is that the increase in sensor data processing leads to a sharp rise in data traffic, which in turn puts pressure on the already scarce radio spectrum. Communication and detection functions share the same radio spectrum, making frequency management more complex and less predictable. In addition, AI is increasingly used in sensor data analysis. Until recently, specific AI systems were mostly deployed on a per-application basis, but the trend is now increasingly shifting towards generative AI systems that combine and interpret different types of data. This raises questions about the ownership, management and use of sensor data. There are also growing concerns about privacy, as sensing technologies can also facilitate unwanted surveillance.

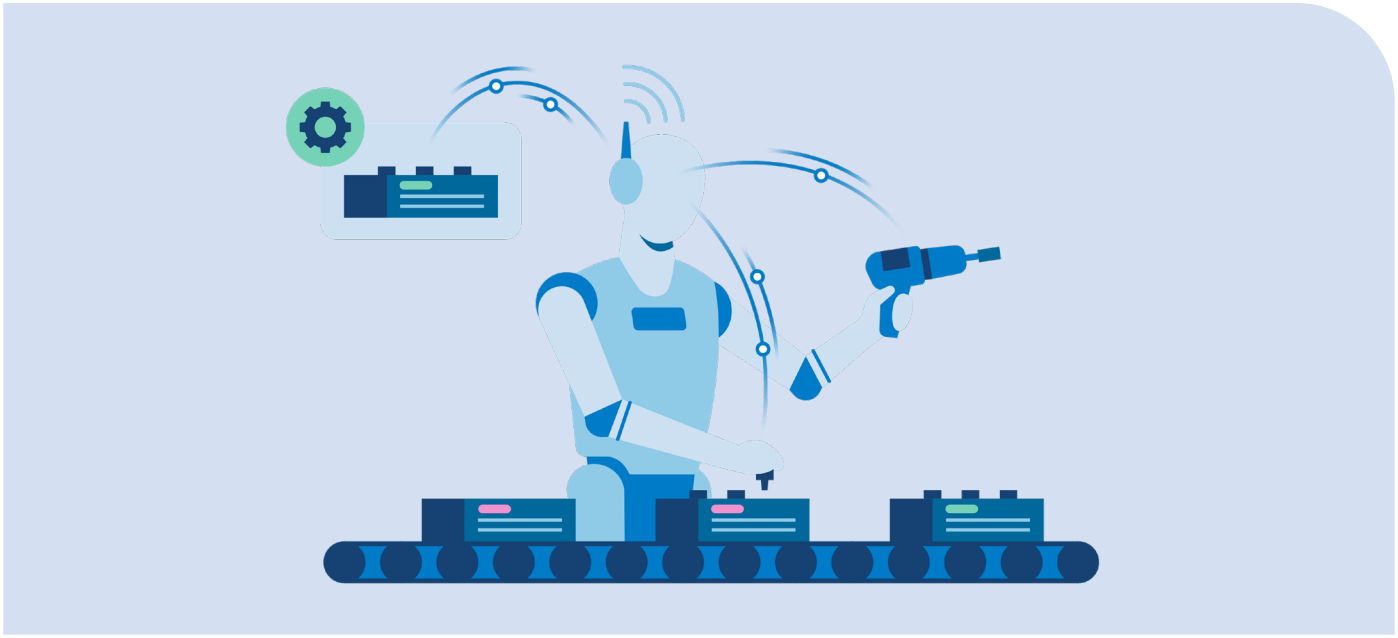
Geopolitical shifts are further driving the development of new sensing technologies, such as drone detection and identification for civilian and military applications. There is also a broader strategic issue at play here: will Europe be able to secure a leading position in the development of quantum and 6G standards, hardware production, or will these sectors once again be dominated by players from China and the United States?

See also

10 AI taking on a physical form

AI taking on a physical form

Impact **medium** Timeframe **0–3 years**



Embodied AI combines sensors, visual data processing ('computer vision') and machine learning algorithms to equip robots, drones and vehicles with the intelligence to perceive their environment, make decisions and act purposefully. The power of embodied AI lies in the interaction between perception, interpretation and control. AI processes data from the environment and uses it to directly control physical systems.

An embodied AI system creates new forms of automation for society. The impact will be different in controlled environments, such as a factory with warehouse robots, than in public spaces. Low-latency connections are crucial for both performance and safety in environments where machines move at high speed and work closely alongside people.

Impact

Where the effects of AI were felt mostly in the digital realm early on, embodied AI is now moving decisively into the physical world, bringing potential risks to the safety of people and property.

The widespread adoption of embodied AI in drones and vehicles is lagging, as the systems still lack sufficient precision and adaptability. As a result, the true impact of this technology will only become fully apparent in the longer term. However, when these systems are deployed at full scale, their heavy reliance on low-latency networks may cause significant network congestion.

AI accelerating scientific practice

Impact **low** Timeframe **> 6 years**



The use of AI technologies is leading to major scientific breakthroughs, such as the sequencing of the human genome, the improvement of climate models by processing of vast amounts of data, and the prediction of protein structures for drug development.

Conversely, the use of AI in science also has certain drawbacks. There are concerns about bias in algorithms, the growing prevalence of hallucinations, phantom references and fabricated data. There is also a risk that the use of AI may erode critical thinking skills.

Scientific progress is expected to accelerate significantly once AI research bots begin conducting research themselves and compare and integrate their findings with those of other bots. This will create a network of bots that accumulate knowledge collectively, much like how this happens within the human scientific community.

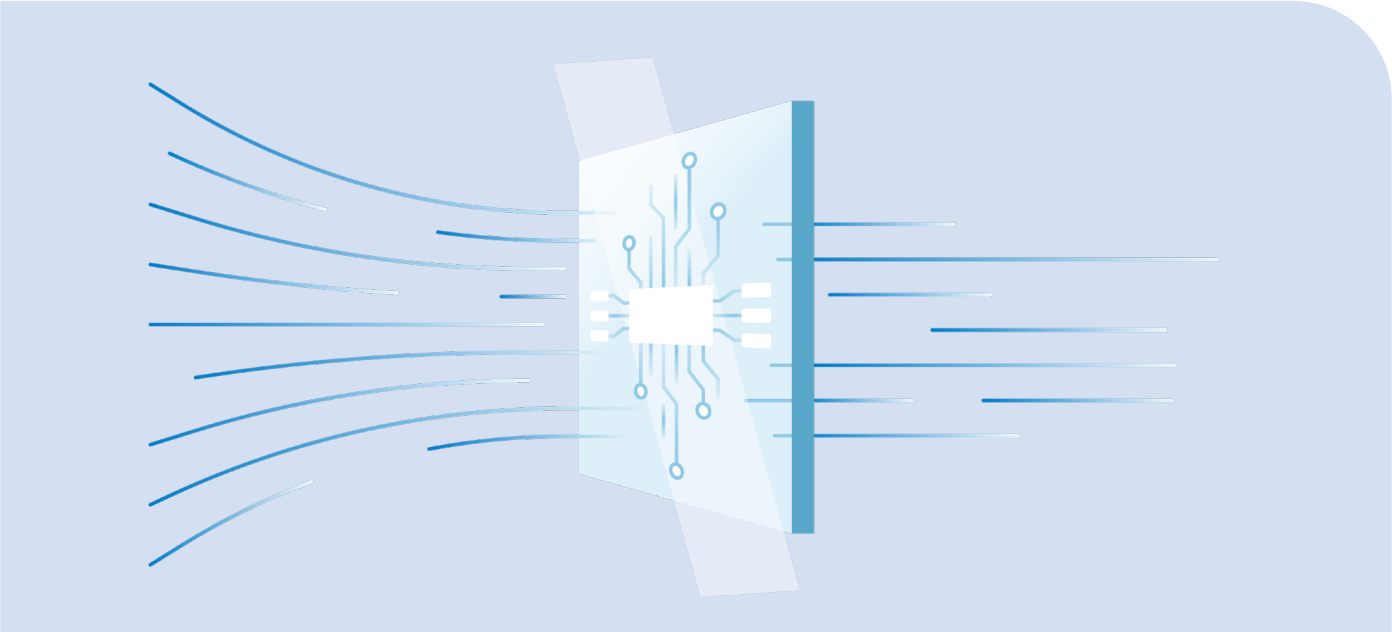
Impact

As with other forms of AI, the effectiveness of research bots will hinge on the availability of data storage, bandwidth and computing power.

Furthermore, providing access to interconnected datasets and jointly funding investments in computers and supercomputers will require close cooperation between educational and research institutions.

Photonic chips

Impact **low** Timeframe **> 6 years**



Photonic chips use light rather than electricity to transmit information. They contribute to a more efficient digital infrastructure by making the transmission of large amounts of data faster and more energy-efficient, as light generates less heat than electrons in copper.
Today, these chips primarily complement traditional electronic chips for short- and ultra-short-range data transmission, which is of particular interest to data centres. In the long term, photonic chips are expected to be capable of performing computations themselves, but this is currently still at the experimental research stage.

Impact

The greatest expected impact lies in the further integration of photonic and electronic chips. The closer optical links are positioned to processors, the faster the data transfer. This can lead to higher data speeds, lower energy consumption and reduced heat generation, enabling data centres to operate more efficiently and sustainably. AI data centres are expected to lead large scale adoption, given the vast volumes of data they process.

DNA-based data storage shows great promise; currently out of reach

Impact **low** Timeframe **> 6 years**



Synthetic DNA storage uses artificially produced DNA to store information, instead of traditional storage media such as hard discs or SSDs. Digital data is converted into a strand of DNA that can later be analysed using DNA sequencing to reconstruct the original digital information.

DNA is suitable for long-term storage of large amounts of data, as it has a high information density and remains stable for thousands of years under the right conditions. We are still a long way away from practical applications, as DNA synthesis and sequencing are still expensive and time intensive. In the future, synthetic DNA storage is expected to be used primarily for archiving data that requires preservation for many years or even centuries.

Impact

The current impact of synthetic DNA storage on the digital infrastructure is limited, as the technology is still too slow and too expensive for everyday use. In the longer term, DNA storage could radically transform the digital infrastructure by offering an alternative to conventional data centres.
DNA offers a storage density millions of times greater than current storage media, enabling vast amounts of data to be stored in an extremely small physical volume. This means that future data centres may require less physical storage space for long-term archives.

At the same time, new demands are being placed on the infrastructure, such as specialised equipment for DNA synthesis and sequencing, automated laboratories, and software that can reliably encode digital files into DNA and decode them again.

Geopolitical developments

Digital infrastructure is taking on an increasingly prominent role in geopolitics, both as a tool and as a target. Various forms of cyberattacks, sabotage and espionage are used to exert influence, gather information or disrupt vital systems. Addressing these threats demands foresight regarding the impact of such threats and measures to mitigate that impact. Digital infrastructure has transformed from a quiet asset into a geopolitical lever, while digital autonomy is gradually taking shape.

Digital infrastructure as a geopolitical lever

Impact **high** Timeframe **0-3 years**



Recently, large scale covert attacks by state actors on the digital infrastructure have increased sharply. These 'hybrid' attacks are growing in number, intensity and diversity. Examples include hacking critical services, disrupting communication signals, sabotaging physical infrastructure, and disinformation campaigns run by hostile states.

The hybrid threat has been steadily increasing in recent years, and this heightened threat level is expected to persist. The Netherlands is in a grey zone: we are not formally at war, but the conditions are not peaceful.

Impact

Cyberattacks can cause widespread outages of essential services such as internet, payment systems or energy supply. Such disruptions can lead to societal destabilisation.

The Netherlands also depends on other countries for critical components of its digital infrastructure. This dependence may increasingly be used as geopolitical leverage, both now and in the future.

The unpredictability of these developments amplifies their impact, as it makes effective preparation more difficult.

See also

16 Cyberattacks becoming more covert and less direct

17 AI increasingly used for cyberattacks and cyber defence

18 Digital autonomy high on the political agenda

19 Growing focus on strategic autonomy in raw materials and semi-finished products

Cyberattacks becoming more covert and less direct

Impact **high** Timeframe **0-3 years**



Although the digital infrastructure is becoming increasingly prominent on the geopolitical stage, the actors behind cyberattacks on this infrastructure are becoming increasingly difficult to identify.

State actors do not carry out attacks directly but use proxies (third parties, such as criminal groups) to do so on their behalf. This makes it more difficult to trace responsibility to the original instigator. Attacks are also becoming more indirect, targeting suppliers or subcontractors within the supply chain. Examples include the SolarWinds attack in 2020, the breach of the Cleo file transfer platform in 2024 and the exploitation of Citrix vulnerabilities in 2025.

Impact

This development increases the vulnerability of the digital infrastructure, as attacks and attackers are harder to trace. Attacks increasingly target the hidden layers of digital infrastructure, making them harder for authorities to detect and counter.

Attacks also attract less attention because SMEs are targeted more often than large companies. Multiple attacks on several smaller firms are far less visible than a single attack on a major organisation.

See also

27 The digital resilience gap between SMEs and large enterprises

AI increasingly used for cyberattacks and cyber defence

Impact **high** Timeframe **0-3 years**



Attackers use sophisticated algorithms to identify, analyse and exploit vulnerabilities. When combined with AI techniques, traditional cyberattacks—e.g., ransomware, viruses and DDoS—become faster, more extensive and harder to detect. AI also lowers the level of technical knowledge and skills required to commit cybercrime. For example, large language models (LLMs) can generate code to carry out cyber crimes and automate attacks.

Effective defence is often only possible using AI technology, such as AI systems that can autonomously repel such attacks and/or identify and address vulnerabilities at an early stage.

Impact

There are already real world examples of AI enhanced adaptive malware and cyber espionage, such as the deployment of LAMEHUG by the Russia linked hacker group APT28 in 2025. A major impact is expected once AI systems are able to operate even more (or fully) autonomously and have the ability to disrupt critical sectors such as telecommunications and energy on a large scale. The complexity and adaptiveness of AI driven attacks leaves organisations less time to address vulnerabilities, making traditional cybersecurity measures obsolete more quickly.

Once AI systems begin conducting attacks independently, it will become even more difficult to attribute responsibility to an instigator. The integration of AI with other technologies such as quantum, satellite and 6G is still in the research phase, but will eventually have a major impact as it further increases the possibilities and speed of attacks.

A positive development is that the Netherlands and the EU have access to computing power and expertise, including in emerging AI factories, research institutes and universities. However, these resources are still only deployed sparingly for resilience.

See also

15 Digital infrastructure as a geopolitical lever

18 Digital autonomy high on the political agenda

19 Growing focus on strategic autonomy in raw materials and semi-finished products

29 Availability of digital infrastructure under pressure

Digital autonomy high on the political agenda

Impact **high** Timeframe **0-3 years**



Current geopolitical tensions call for measures that will give Europe greater control over strategic dependencies within its digital infrastructure. This challenge is becoming more urgent, as the United States and China are ahead of Europe when it comes to the development of key digital technologies such as AI and quantum technology.

Digital standards are also increasingly originating in Asia, particularly in China and India. The standards from these countries are often aimed at promoting their own industries. This will lead to a decline in European and Dutch influence and may put European companies at a disadvantage.

To reduce dependence on non-European technology, European and Dutch governments and the business community are pursuing greater digital autonomy, backed by a robust European and Dutch political agenda.

This new focus also presents opportunities to develop national and European initiatives and improve the investment climate. One example of this is Gaia-X, a European initiative to develop a federated data and cloud infrastructure.

Impact

Problematic dependencies on digital infrastructure by state or non state actors can lead to interference and increase the risk of outages, disruptions or sabotage. However, complete independence from non-European countries is neither feasible nor desirable. Conversely, the production of European resources that are highly sought after outside Europe offers a significant strategic advantage.

The European digital autonomy agenda will lead to a more conscious assessment of risks and to an active commitment to the resilience of our own systems.

Growing focus on strategic autonomy in raw materials and semi-finished products

Impact **high** Timeframe **3-6 years**



We are dependent on long, complex, global supply chains for strategic raw materials and critical technologies such as rare metals needed for producing fibre optic cables or chips, as well as the chips themselves. Specific links within these chains are controlled by particular countries. Taiwan, for example, dominates chip production (TSMC), while China holds many of the critical raw materials required for manufacturing chips and batteries.

In June 2026, the Dutch government published the Dutch Critical Raw Materials List. This initiative underscores the importance of strategic autonomy for these materials.

To increase autonomy, efforts will focus on using European alternatives where possible, diversifying and strengthening the Netherlands' competitive edge, and recycling and circular use of materials.

Impact

Dependence on a small number of countries and companies makes the digital infrastructure vulnerable to geopolitical tensions, trade restrictions and supply chain disruptions. This can put the availability and maintenance of networks, data centres and telecom services under pressure.

Shortages of semiconductors, fibre optic components or other essential parts can cause delays in the construction, replacement and further development of digital infrastructure, increasing the risks to the continuity of critical digital services.

Foreign interference undermining earning capacity in the Netherlands

Impact **medium** Timeframe **3-6 years**



Economic security refers to the resilience of our economy against interference and the abuse of economic activities for geopolitical purposes. Such activities can pose a risk to national security. Foreign companies or investors acting out of geopolitical interests may gain access to sensitive information, technology, innovations and business processes. This can be through espionage, but also through acquisitions of or investments in enterprises possessing strategic knowledge or technology, or that occupy a crucial position within critical infrastructure. This occurs in both the European and Caribbean parts of the Netherlands. We risk losing strategic knowledge and competitiveness and becoming more dependent on foreign parties and supply chains, which could in turn lead to both economic and political dependence over the longer term.

Impact

Strategic dependencies can leave digital infrastructure trailing in innovation and knowledge development. Once we start falling behind, it is hard to catch up—or even impossible in the long run.

See also

18 Digital autonomy high on the political agenda

19 Growing focus on strategic autonomy in raw materials and semi-finished products

22 Legislation in a bind between risk management and digital innovation

Societal developments

Societal developments include political, economic, social, ecological and legal changes that have an impact on the organisation of our society and our daily lives. We can see a wide variety of such developments through the lens of digital infrastructure. For example, we highlight the indispensable role of the digital infrastructure in keeping society functioning, while at the same time, changes in regulatory pressure, climate change and labour market shortages create new challenges for the digital infrastructure itself.

Legislation in a bind between risk management and digital innovation

Impact **high** Timeframe **0-3 years**



The growing body of European legislation such as the GDPR, NIS2, DORA, the Data Act and the AI Regulation is making compliance increasingly complex and costly. This weakens our competitive position and creates market imbalances. Larger companies with substantial financial resources can easily absorb compliance costs, while smaller organisations are heavily burdened. The business community is therefore calling for reduced regulatory pressure. Governments are responding to these calls, and the European Union is working to simplify regulation.

At the same time, these regulations are essential for a safe and reliable digital society. Legal requirements related to cybersecurity, privacy and fundamental rights help build confidence in digital systems and form an important prerequisite for responsible innovation.

Impact

The simplification of regulations can lead to less effective mitigation of risks associated with the use of digital technologies.

In addition, an unpredictable legislature makes it harder for companies to anticipate what they must comply with and how legislation will develop in the future.

In the Caribbean Netherlands, a direct transposition of the above-mentioned European legislation is often lacking, meaning that changes in regulatory pressure may not be equally applicable.

See also

5 Growing demand for radio spectrum driving scarcity and vulnerability

11 AI accelerating scientific practice

15 Digital infrastructure as a geopolitical lever

20 Foreign interference undermining earning capacity in the Netherlands

27 The digital resilience gap between SMEs and large enterprises

Digital infrastructure interwoven into every aspect of our lives

Impact **high** Timeframe **0-3 years**



Dependence on digital infrastructure is increasing as more and more systems, processes and devices are connected to it, from energy and water supply to payment systems and communication. This trend has been underway for many years, and the ever-increasing integration into our personal, everyday lives is particularly noteworthy.

Dealing with the growing dependence on the digital infrastructure is one of the biggest challenges of the present and the near future. There are many future scenarios conceivable, ranging from further stimulation of digital growth by authorities and the business sector, to greater fragmentation of the digital landscape due to geopolitical developments and public resistance.

We are already seeing societal movements that consciously focus on increasing independence from digital infrastructure. This is expressed through a greater focus on autonomy, self reliance and the search for technological alternatives. Recent geopolitical and cultural developments demonstrate on a small scale that there is growing interest in analogue or autonomous alternatives, such as decentralised and local networks, microgrids and home batteries.

We are also seeing society's dependence on digital infrastructure reach its limits in other ways, due to a lack of space, water or energy.

Impact

The strong interdependence between digital infrastructure and social and economic processes amplifies the impact of disruptions, extending deep into people's personal lives. The failure of a single component can trigger a chain reaction in other sectors and processes.

See also

15 Digital infrastructure as a geopolitical lever

18 Digital autonomy high on the political agenda

22 Legislation in a bind between risk management and digital innovation

Synthetic identities increasing pressure on digital trust frameworks

Impact **medium** Timeframe **< 3 years**



The tsunami of information generated by AI presents a new challenge to trust in the digital world. Where media such as photos and videos were previously often merely 'tampered with', media can now be constructed from scratch quickly and realistically. Digital identity is one area significantly affected by this. 'Deepfakes' are increasingly being generated using AI and used to forge digital identities to commit identity fraud. Fully AI-generated (synthetic) identities are also becoming increasingly common.

Impact

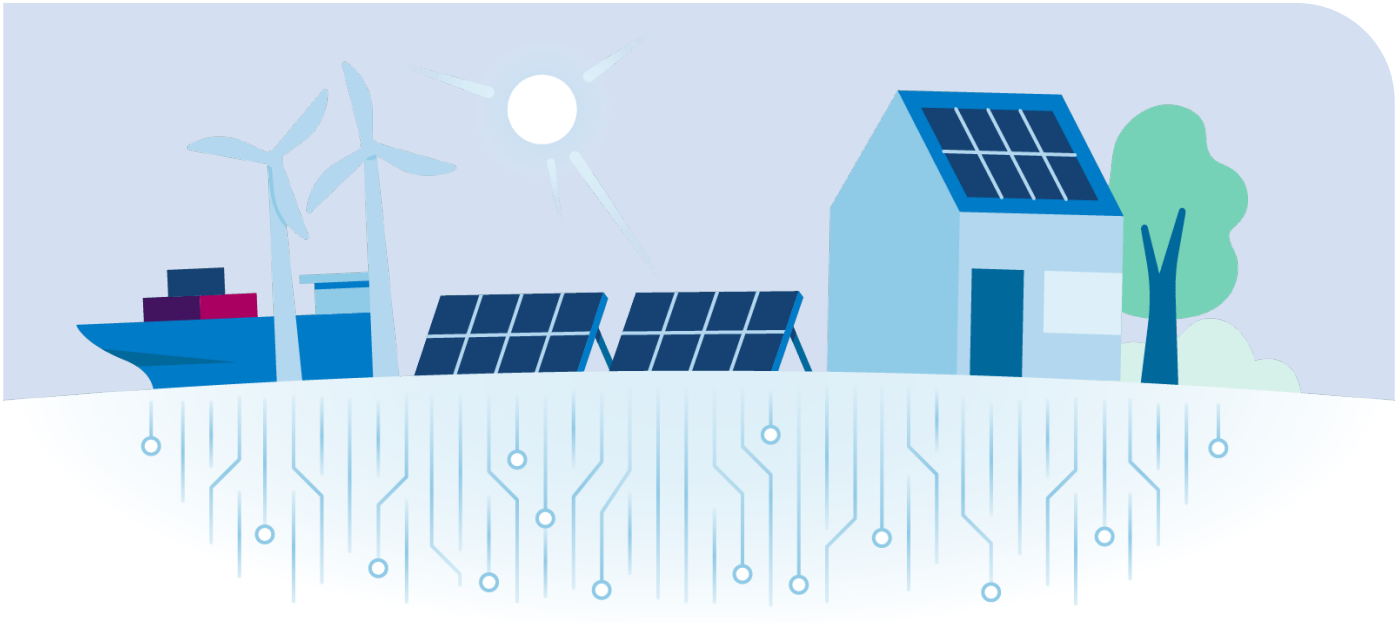
It is becoming increasingly difficult to establish the authenticity of digital information, while at the same time, the use of digital identities is on the rise.

Digital provenance is being explored as a potential solution to the increasing volume of AI-generated content. Digital provenance involves recording a file's origin and revision history in its metadata. This requires broad acceptance of technical standards, as well as a balance between the privacy of those involved and transparency about how a file was created.

The growing role of digital identity is reflected in social and political debates on topics such as online anonymity and age verification on social media. The revised eIDAS regulation addresses this. By the end of 2026 at the latest, all EU Member States must offer a digital wallet that enables residents to securely share identity attributes online, such as confirmation that they are over 18 years old.

Growing demand for energy and water

Impact **medium** Timeframe **< 3 years**



The rapid expansion of data centres, high power IoT, 5G/6G and AI is driving substantial growth in energy and water consumption. This strains electricity grids and intensifies competition with other sectors for grid access. A stronger focus on redundancy will increase consumption even further.

Water shortages are causing constraints on both the use of digital infrastructure and the production of new components (chips and hardware). Digital infrastructure also faces competition from other sectors, including drinking water supply and agriculture, particularly in South Holland.

Impact

The growing demand for energy is leading to shortages and outages as grids become overloaded. This trend puts pressure on the availability, continuity and growth of the digital infrastructure. Conversely, digital infrastructure outages also disrupt the continuity of the electricity supply.

Competition for new connections is increasing (e.g., between data centres and residential developments) leading to a deterioration in the business climate. The increasing pressure on the energy supply is also reflected in high energy costs for data centres and networks, potentially resulting in price hikes for end users.
Lastly, the current reliance on fossil fuels for electricity generation entails a geopolitical risk.

This development also exacerbates inequality, as only end users with sufficient resources and space for backups (e.g., fuel and batteries) can sustain themselves in the event of an outage.

One potential positive impact of the need for more efficient use of energy, water and raw materials is that it encourages the development of advances such as more energy-efficient networks, more efficient chips and neuromorphic computing.

See also

12 Photonic chips

31 Weather extremes increasing vulnerability of digital infrastructure

Influx of non-compliant equipment increasing safety risks

Impact **medium** Timeframe **0-3 years**



Since the coronavirus pandemic, a difficult-to-manage stream of individual e-commerce parcels has emerged alongside the regular container flows. These parcels often enter the EU via less stringent customs checks. As a transit country, the Netherlands has a pivotal role in this, with more than 1 billion parcels crossing its borders each year since 2024.

Customs declarations for these parcels are often incorrect or incomplete, meaning that regulators have limited insight into the contents. Between 85 and 95% of the products do not comply with EU regulations, such as those concerning cybersecurity.

An EU levy on parcels has been in place since 1 July 2026. This is likely to lead to a slight decline in the number of individual parcels sent. At the same time, however, VLOPS ('very large online platforms', such as major international online retailers) will increasingly use distribution centres within the European Union. This will result in a shift in the flow of parcels, but not necessarily a reduction in volume.

Impact

The influx of non-compliant products (e.g., wireless-enabled equipment and IoT devices) is increasing interference in the radio frequency spectrum. Interference can also impact critical systems, including emergency service communications. Safety risks for consumers are also increasing, including fire hazards from unsafe chargers, vulnerabilities caused by devices containing malware and exposure to harmful substances.

See also

27 The digital resilience gap between SMEs and large enterprises

The digital resilience gap between SMEs and large enterprises

Impact **medium** Timeframe **0-3 years**



SMEs, like large enterprises, operate within supply chains that are critical to the digital infrastructure. However, cyber resilience is lagging among SMEs—especially regarding more complex measures like data encryption—while the number of cyberattacks on SMEs is on the rise. This growing gap in cyber resilience between SMEs and large enterprises increases the vulnerability of critical systems. This is particularly relevant for businesses that fulfil critical functions within the supply chain.

Impact

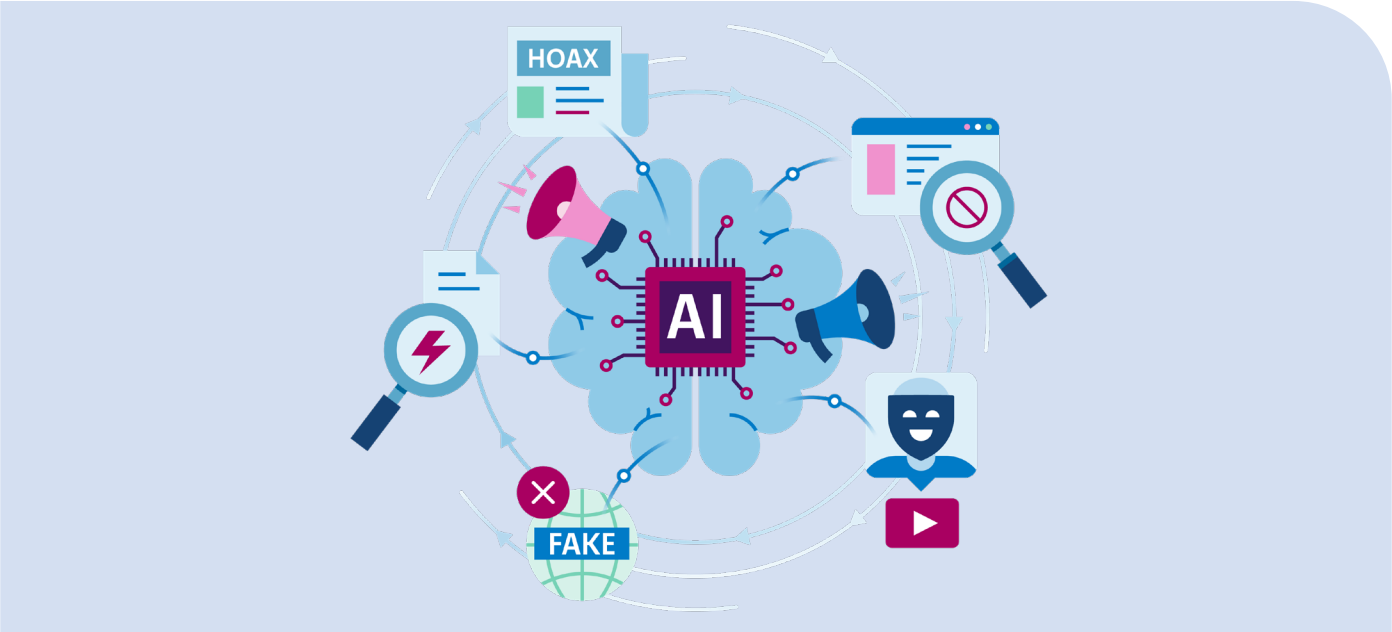
SMEs are a key component of the Dutch economy and the digital infrastructure. Structural shortcomings in digital resilience among SMEs increase the vulnerability of the entire digital infrastructure.

See also

29 Availability of digital infrastructure under pressure

The vicious cycle of AI and disinformation

Impact **medium** Timeframe **0-3 years**



Generative AI enables the rapid, low cost and large scale creation and targeted dissemination of convincing but misleading text, images and audio. Disinformation from online influence campaigns can end up in AI training data or information sources, prompting AI systems to reproduce the misleading material.

Impact

Disinformation has no direct impact on the digital infrastructure itself, but can affect the use of that infrastructure by undermining public trust in digital services, government communications or online information provision, for example.

See also

15 Digital infrastructure as a geopolitical lever

Availability of digital infrastructure under pressure

Impact **high** Timeframe **3-6 years**



The Netherlands boasts high levels of availability and accessibility for its critical infrastructure (> 99.98%). The question is whether these levels can be maintained, given the strong increase in hybrid threats that disrupt digital infrastructure.

This is why there is a call to invest in robust and resilient digital services. This is not the same as guaranteeing that digital services are continuously available; robustness and resilience increase the ability to cope with disruptions and to safeguard the continuity of critical services during such events.

This development marks a break with current policy and the public expectation that digital infrastructure is always available and accessible. Calls for preparedness can help ensure that users perceive outages less as disruptions and more as incidents to be expected.

Impact

The quality and continuity of the digital infrastructure will become less of a certainty. Specific parties may be prioritised in terms of availability, as is currently the case with electricity. This could undermine expectations regarding the reliability of the infrastructure. This may also create a digital divide between those with stable access to the digital infrastructure and those without. It could also affect broader public confidence in digital systems and the
Netherlands' competitive position. In the Caribbean Netherlands, expectations regarding availability are already different due to limited redundancy and more frequent threats from weather conditions.
This trend may fuel the demand for analogue alternatives, which will in turn lead to greater redundancy.

See also

5 Growing demand for radio spectrum driving scarcity and vulnerability

27 The digital resilience gap between SMEs and large enterprises

Shortage of professionals straining availability and innovation

Impact **medium** Timeframe **3-6 years**



The persistent shortage of IT professionals is expected to continue in both the short and long term, as enrolment has stagnated in both secondary and higher education. The shortage is exacerbated by demographic developments: as the population ages, experienced professionals leave the workforce, with fewer young people joining it to replace them. There are also concerns about the quality of the inflow, with declining PISA scores in reading, mathematics and science.

Automation, particularly AI, can take over certain IT work and partially offset shortages. At the same time, AI primarily takes over junior IT tasks, which limits progression into senior roles and ultimately leads to shortages of experienced IT professionals.
The Netherlands can attract national and international professionals with relatively high salaries. It remains uncertain whether this—in combination with automation—will be sufficient to address the shortage.

Impact

Maintaining the digital infrastructure is likely to become more challenging with the limited number of professionals available, ranging from maintenance technicians to cybersecurity specialists. We also run the risk that the focus will shift to only carrying out essential maintenance and 'putting out fires', while structural innovation is moved to the back burner.

See also

29 Availability of digital infrastructure under pressure

Weather extremes increasing vulnerability of digital infrastructure

Impact **medium** Timeframe **> 6 years**



The growing frequency and unpredictability of extreme weather events is undermining the reliability of energy supplies and digital connectivity. It is precisely at such times that reliable communication is vital.
Extreme rainfall, heatwaves, high winds and ground subsidence can damage data centres, transmission masts, cables and electricity infrastructure, leading to communication outages, cooling system failures, overheating and data loss.
The risks vary by region. In the European Netherlands, the main concerns are flooding, heat and storm damage, The risks are greater in the Caribbean Netherlands due to the geographical location and exposure to extreme weather. Hurricanes have already led to outages of essential, and in some cases all, communication on the islands.

Impact

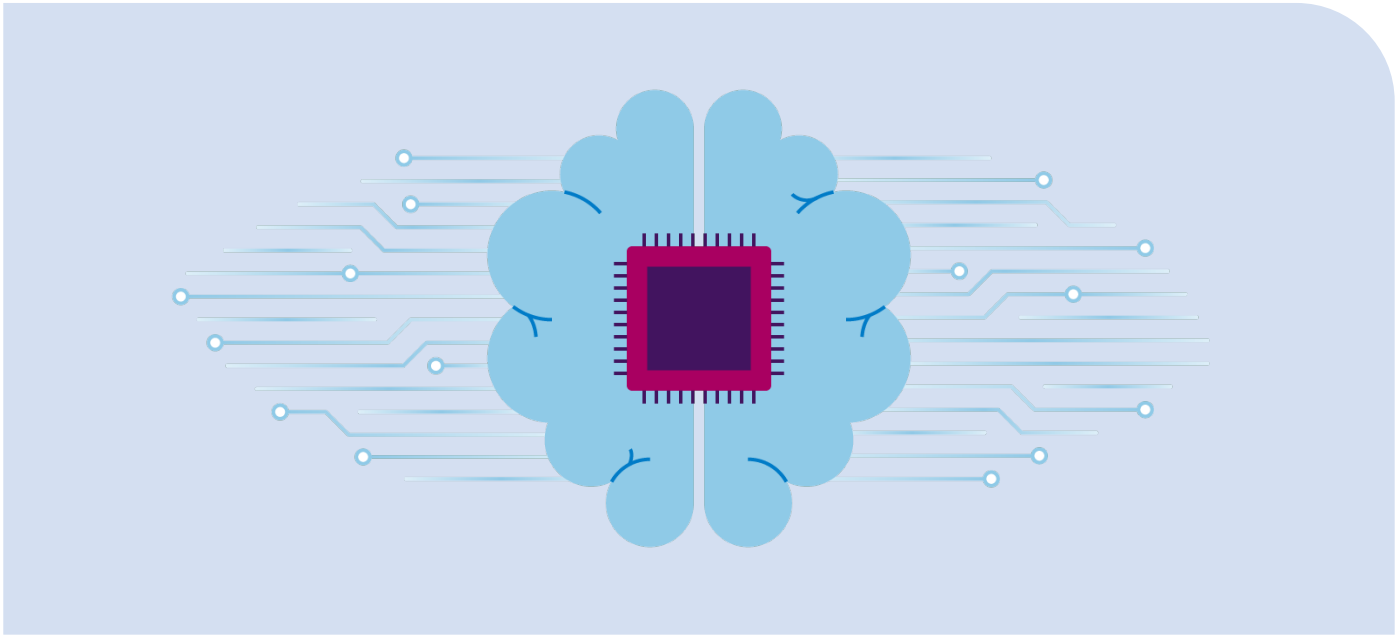
In the European Netherlands, the greatest risk of flooding is near rivers and below sea level (NAP), where the majority of data centres are located. In the event of storm damage to antennas, replacement equipment is either unavailable or in very short supply. This results in large-scale outages of digital infrastructure, with potentially long recovery times.
In the Caribbean Netherlands, hurricanes, rising sea levels and erosion increase the vulnerability of the telecommunications infrastructure. Redundancy is limited: damage to a single submarine cable or transmission mast can take entire sections of the islands offline. Wind and lightning can damage transmission masts and satellite links, causing failures in digital infrastructure that impact the economy and critical sectors.
Data centres are scarce, but are equipped with diesel generators and backup batteries. Recovery can take a long time due to limited logistics and supplies. The increasing vulnerability calls for investment in the telecommunications infrastructure to ensure its continuity.
Innovative solutions such as hurricane-proof transmission masts, satellite-based backup, microgrids powered by renewable energy, stockpiles of critical components, and water-resistant or floating data centres can enhance resilience.

See also

29 Availability of digital infrastructure under pressure

New human machine interfaces

Impact **low** Timeframe **> 6 years**



The way people interact with the digital world is changing. Today, we still primarily access it through the glass screens of smartphones and tablets, staring at them while swiping and tapping. But new interfaces are emerging. Technologies such as augmented reality (AR), virtual reality (VR), mixed reality (MR) and neurotechnology mark a fundamental shift in how humans interact with technology.

AR, VR and MR supplement or even replace physical reality with digital objects and environments. These technologies are already commercially available but have not yet been widely adopted, apart from niche applications such as head up displays in cars or in video games. This is expected to change in the longer term, as major companies are investing heavily in these technologies.

The same applies to neurotechnology, which enables direct communication between the brain and machines and, over time may offer ways to influence human behaviour or cognitive processes. Current applications are mostly in the medical domain, but neurotechnology could be ready for introduction into consumer products in the medium term.

Impact

Large-scale brain-to-machine interfaces are not expected for the foreseeable future due to technological limitations and social and ethical issues. There are also significant legal issues, as neurotechnology is not yet explicitly covered by legislation relating to AI, privacy or product safety.

Neurotechnological applications and advanced AR/VR systems, including AI-driven real-time translation, object recognition and behavioural analysis, also place heavy demands on the underlying digital infrastructure. These applications and systems rely on fast and reliable 5G and future 6G networks, combined with local data processing ('edge computing') to minimise latency. This development also places higher demands on system security to protect privacy-sensitive data.

One major risk associated with advanced human-machine interfaces is their vulnerability to cyberattacks. As a result, governments are placing greater emphasis on regulating neurotechnology. For example, in 2021, Chile became the first country to introduce specific legislation to protect neurological data. In Europe, research is being conducted into how neurotechnology fits within existing frameworks such as the GDPR and the AI Regulation.

See also

23 Digital infrastructure interwoven into every aspect of our lives

Conclusion

This fifth edition of the Trend Radar outlines 26 developments that we expect to shape the digital infrastructure over the next ten years. These developments require constant attention and adaptability. RDI continuously factors these developments into its regulatory activities. Whether it concerns the impact of AI, the vulnerability of undersea data cables or the increasing pressure on energy supplies, it is essential that we take the right steps now. While this report highlights the developments on the radar, it is up to all of us to translate them into policy, investment and collaboration.

This Trend Radar was made possible by the contributions of numerous experts, stakeholders and colleagues, both internal and external to the RDI. We would like to thank everyone who contributed.

If you have questions or ideas or want to continue the conversation, please get in touch via trendradar@rdi.nl

References

- ABN AMRO - Mkb vaker doelwit van cybercrime dan grootbedrijf
- Adviescollege toetsing regeldruk (ATR) - ATR opent meldpunt signalen regeldruk
- AIVD - Dreigingsbeeld Statelijke Actoren 2025
- AIVD - Tussen vrede en oorlog. De oorlog in Oekraïne en de Russische dreiging in Europa
- Allianz - Code, carbon, kilowatts: AI's hidden toll and the race to green the grid
- Centraal Bureau voor de Statistiek (CBS) - Datacenters verbruiken 4,6 procent van de elektriciteit
- Centre for Emerging Technology and Security (CETaS) - Adding Fuel to the Fire: AI Information Threats and Crisis Events
- Centre for Emerging Technology and Security (CETaS) - Beyond Spam Bots: The Rise of AI-Powered Disinformation Machines and the Imperative for Strategic Response
- Clingendael - Nederland en de EU: Benoem, bescherm en beheer strategische digitale infrastructuur
- College voor de Rechten van de Mens - EU-wetswijzingen 'digitale omnibus' zorgelijk voor grondrechten
- Cyber Security Raad (CSR) - AI als wapen bedreigt digitale veiligheid
- Denk vooruit - Uitval telecommunicatie
- Digital Forensic Research Lab (DFRLab) - Russia-linked Pravda network cited on Wikipedia, LLMs, and X
- Europese Commissie - Space Traffic Management
- Gaia-X Hub the Netherlands
- Joint Research Centre (JRC) - The Role of Artificial Intelligence in Scientific Research
- KNMI - KNMI'23-klimaatscenario's
- Nationaal Coördinator Terrorismebestrijding en Veiligheid (NCTV) - Cybersecuritybeeld Nederland 2025
- Nationaal Cyber Security Centrum (NCSC) - Anthropic's frontiermodel Mythos vraagt om directe actie
- Nationaal Cyber Security Centrum (NCSC) - Cybersecuritymonitor 2025: minder cyberaanvallen, weerbaarheidskloof blijft
- Nationaal Groeifonds - Creative Industries Immersive Impact Coalition (CIIIC)
- Nationaal Groeifonds - PhotonDelta
- Planbureau voor de Leefomgeving (PBL) - Strategische autonomie vraagt om regio- en bedrijfstakspecifiek beleid
- Planbureau voor de Leefomgeving (PBL) - Voorbij de risico's: keuzes voor een klimaatbestendige leefomgeving
- Radboud Universiteit - De toekomst van dataopslag schuilt in microbolletjes met DNA
- Rathenau Instituut - NeuroTechnology
- Rijksinspectie Digitale Infrastructuur (RDI) - Toepassingen van 6G
- Rijksoverheid - Economische veiligheid | Maak je bedrijf weerbaar
- Rijksoverheid - Nieuwe visie legt fundament voor een autonome en soevereine digitale overheid
- Rijksoverheid - Ruimtelijk Ontwikkelingsprogramma Caribisch Nederland
- Rijksoverheid - Themarapportage Rijksbrede Risicoanalyse Caribisch deel van het Koninkrijk der Nederlanden
- Rijksoverheid - Verkenning van het raakvlak van cybersecurity en AI
- Sociaal-Economische Raad (SER) - Digitalisering: kansen en risico's
- Tweede Kamer der Staten-Generaal - Economische Veiligheid
- Tweede Kamer der Staten-Generaal - Kabinetsinzet nationale grondstoffenstrategie
- Tweede Kamer der Staten-Generaal -Nationale handling fee op e-commercezendingen
- UWV - ICT-beroepen in beeld
- Wetenschappelijke Raad voor het Regeringsbeleid (WRR) - Markt, overheid en strategische autonomie

Meer lezen op de website van RDI

- Rijksinspectie Digitale Infrastructuur (RDI) - De route naar digitale autonomie
- Rijksinspectie Digitale Infrastructuur (RDI) - Elektronische vertrouwensdiensten
- Rijksinspectie Digitale Infrastructuur (RDI) - Kunstmatige intelligentie (AI)
- Rijksinspectie Digitale Infrastructuur (RDI) - Nederlandse toezichthouders: gezamenlijke aanpak e-commerce producten nodig om consumenten te beschermen
- Rijksinspectie Digitale Infrastructuur (RDI) - Onderzoek dynamisch spectrumgebruik
- Rijksinspectie Digitale Infrastructuur (RDI) - Quantumcomputers en digitale weerbaarheid: waarom organisaties nu al moeten handelen

■ in Dutch

This is a publication by
Dutch Authority for Digital Infrastructure
Ministry of Economic Affairs and Climate Policy

Emmasingel 1 Groningen
088 - 041 60 00
info@rdi.nl
www.rdi.nl

September 2026

#wijzijnRDI