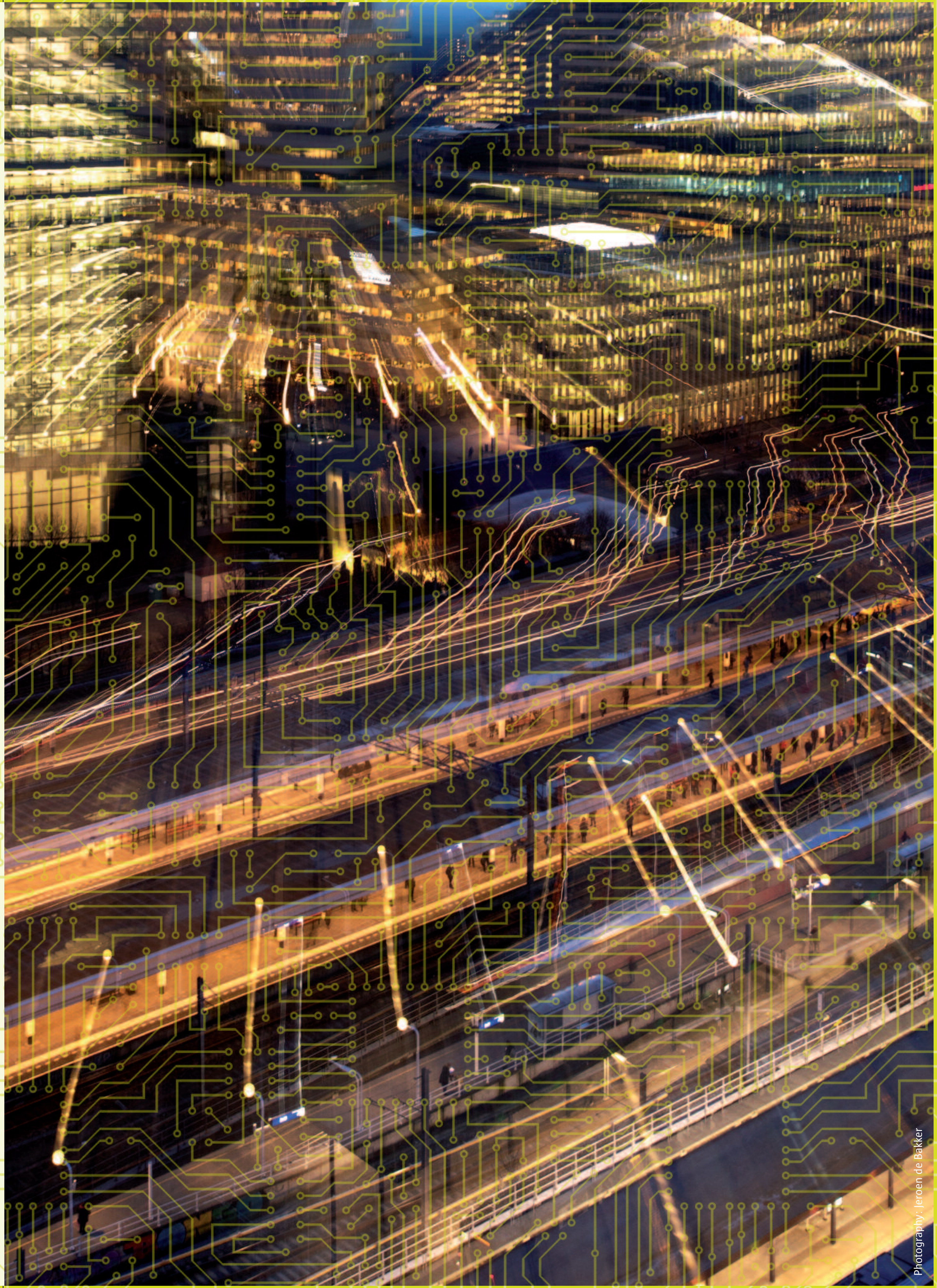
CSR Cyber Security Council

CSR MULTIANNUAL STRATEGY 2018–2021

> *“The future depends on what you do today”*
>
> *Mahatma Gandhi (1869-1948)*



Photography: Jeroen de Bakker

INTRODUCTION

As the home of one of the largest internet hubs of the world and superfast telecom networks for broadband, the Netherlands is at the forefront of digitalisation. As a result, our economy currently ranks as the fourth most IT-intensive economy in Europe, and seventh in the world (2017). If we wish to maintain this digital position, we cannot afford to sit still. The number of cyberattacks is on the rise across the globe, with the Netherlands remaining an attractive target for actors. Even so we are still not seeing politicians, boardroom members, entrepreneurs and citizens respond with the necessary sense of urgency in each case. The level of awareness and the sense of urgency are too low in our country, and the human element in particular is proving to be a weak link in cybersecurity.

This is why the CSR has made a conscious effort over the past few years to put cybersecurity on the agenda in the Netherlands in both the public and private domains. On the one hand, it has done so by issuing advice and commissioning research. On the other hand, it has promoted awareness by raising cybersecurity topics in the media. Examples include recommendations such as 'Cybersecurity in the education and private sectors', 'Towards a nationwide system of information exchanges' and ‘Towards a safe, connected, digital society’, and also reports such as The Internet of Things: opportunities, threats and measures' and 'The economic and social need for more cybersecurity, keeping "dry feet" in the digital era'. In addition, the CSR has held boardroom meetings at various Dutch organisations to put the urgent need for cybersecurity on the agenda and continues to organise further meetings and seminars to open a dialogue with boardroom members on topics related to cybersecurity. And lastly the CSR is promoting the establishment of similar councils with a membership drawn from the public, private and scientific sectors in other EU countries. Efforts by the council in this regard include talks held in Denmark and Belgium.

But there remains more for us to do. The use of digital technologies will continue to increase worldwide over the coming years, which in turn will increase our dependence on IT. This will represent tremendous opportunities for the Netherlands as a society and as an economy. Cybersecurity will be key to our ability to seize these opportunities and this requires (continued) investment on our part. The government has set structural investment in cybersecurity at 95 million euros, which amount which is split between various departments. Work will be facilitated through an ambitious cybersecurity agenda, which focuses on topics including standards for IoT devices, the promotion of cybersecurity research and the improvement of information campaigns around cyber hygiene.

It is essential for the public to have confidence in society and social structures. The Netherlands must (continue to) function as a secure, open and prosperous society. Maintaining our digital position remains a priority and requires that our government, politicians, policymakers, boardroom members, supervisory bodies, businesses and citizens engage with this on a structural basis.

Everyone shares in the responsibility to protect our economy, prosperity and society. This demands central coordination, an area in which the government must lead, including by setting the example. Citizens and businesses must be able to transact safely online with the government.

It is equally important that the private sector must ensure they get the basics right. Cybersecurity is a boardroom responsibility. Companies must protect their own networks and ensure they have the capacity to defend against cyberattacks. The council therefore advises that at least 10% of the IT budget is set aside for cybersecurity.

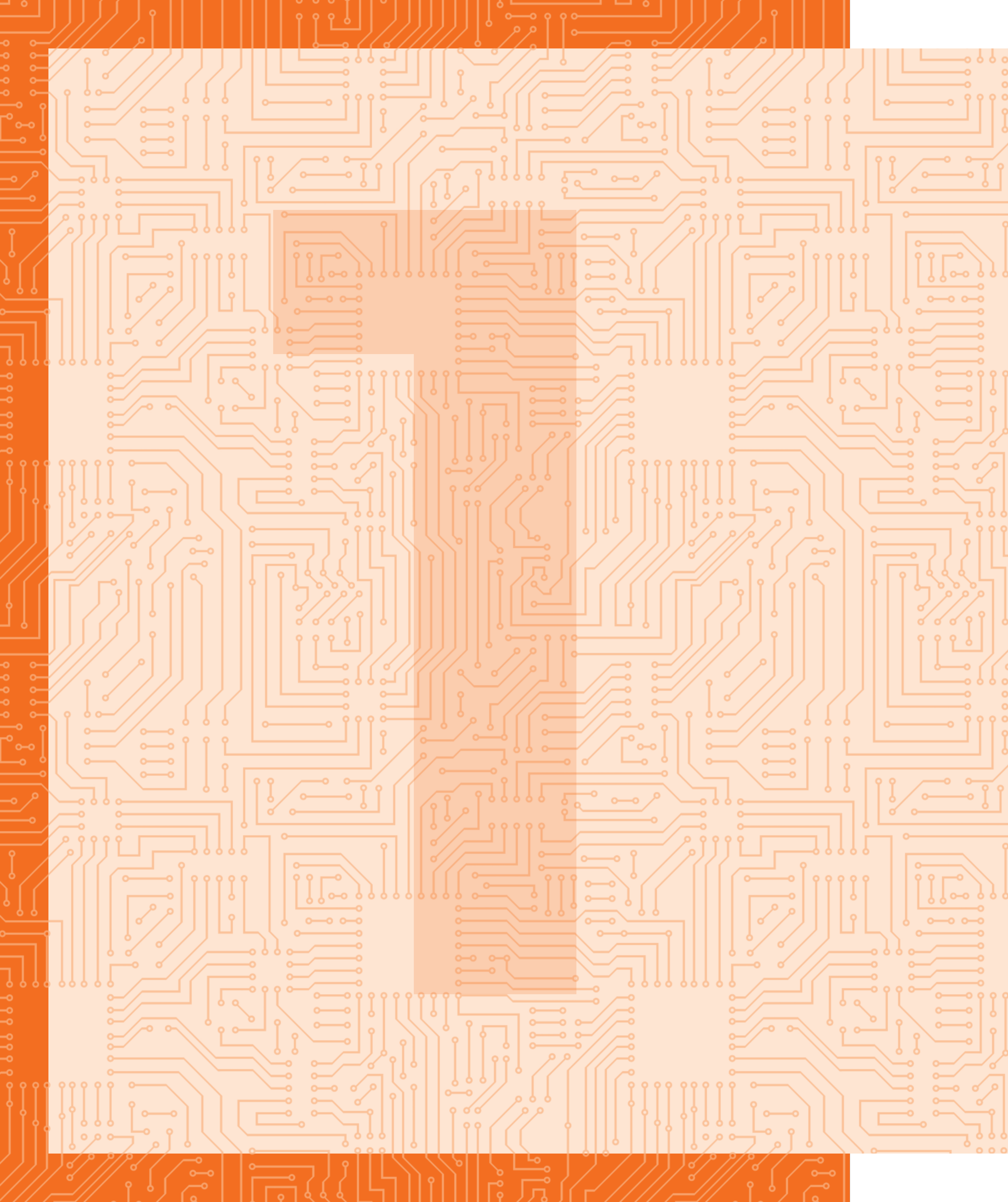
And lastly there is also an expectation on citizens to exercise a certain measure of cyber sensibility and take their share of the responsibility. Public authorities work with the business community to facilitate these efforts by strengthening their digital proficiency, and by emphasising the responsibility that public and private sector organisations have towards their users. The council also calls for special attention to be paid to young people, who hold the key to our future. The curriculum in both primary and secondary education must include a structural focus on developing digital competency in young people. There has also to be a greater focus on cybersecurity and on career avenues in this field, in order to reduce the growing shortage of cybersecurity professionals. The CSR promotes this through the annual National Cyber Security Summer School, which launched in 2016.

In summary, there is a lot to do in order to safeguard the digital leadership position of the Netherlands. The CSR, which has already launched a great many actions in support of this in previous years, will continue to do so in the years to come. We will actively work each year to improve awareness and digital resilience in our country. Over the coming years the council will dedicate its efforts to a number of strategic themes that specifically target cybersecurity, including supervision and guidance, growing dependence on (digital) technologies, enforcement and monitoring, and new technologies. The CSR Multiannual Strategy will tell you how we arrived at these themes.

At the same time, it is key to remember that the cyber landscape is in a constant state of flux. This never-ending rat race requires us to be vigilant and prepared for all possible scenarios at all times. This is no less true for the council. Since our agenda is shaped by current events, the CSR Multiannual Strategy 2018-2021 will be a living document that we will supplement and adapt as required in order to reflect current trends.

On behalf of the Cyber Security Council,

Dick Schoof, co-chairman,
Jos Nijhuis, co-chairman



MISSION, VISION AND STRATEGY

The Cyber Security Council (CSR) is a national and strategic advisory body to the government and, through the government, to the business community. The council is made up of highly-placed representatives in public, private and scientific organisations. The CSR works at a strategic level to increase cybersecurity in the Netherlands.

1.1 Mission

The council contributes to openness, security and prosperity in the Netherlands as a digital nation, by providing cybersecurity-related advice to the government and, through the government, to the private sector.

1.2 Vision

Through its work, the council will contribute to the Netherlands' objective of being an open and secure nation with a thriving digital economy. The aim of the council's efforts is to increase resilience against cyberattacks in the Netherlands and capitalise on the opportunities offered by a secure digital economy.

1.3 Strategy

The council will invest in the effectiveness of its recommendations. Its members will be given strategic roles to enhance the impact of recommendations. Examples of this include acting as spokespersons to the media and monitoring the take-up of recommendations issued. The CSR will deliver impact by matching each topic with a fitting method. The council has a wide range of methods at its disposal ('standard' recommendations, guidelines, discussions and meetings), which it employs in a considered manner. The council will also closely monitor the impact of its products and recommendations. The CSR will action this by drawing up a strategic plan that will allow the council to keep close track of the extent to which its products and recommendations are contributing to a secure, open and prosperous society.

1.4 The council's terms of reference

The council has three tasks that will enable it to achieve its mission. The implementation of these tasks will be based on the following starting principles:

1. The council will act strictly as an initiator; it will not structurally concern itself with the implementation of initiatives.
2. The council will provide advice to the government and, through the government, to the private sector, as regards strategic topics in the area of cybersecurity. Its recommendations serve to set a direction and encourage parties to take action. The target audiences of the recommendations are the government and the private sector (rather than individual businesses).
3. The council not only compiles 'standard' recommendations; it also utilises other products and activities, including guidelines, discussions and meetings.

The council's terms of reference:

1. **Providing solicited and unsolicited strategic advice on cybersecurity to the Dutch government and the private sector (through the government).**
2. **Monitoring trends and new technological developments and, where necessary, translating these into potential measures to reduce the cybersecurity risks and to increase the economic opportunities.**
3. **Initiating and/or accelerating relevant initiatives in the Netherlands and in the European Union that demonstrably contribute to raising the level of cybersecurity in the Netherlands.**

Re 1 Providing solicited and unsolicited strategic advice on cybersecurity to the Dutch government and the private sector (through the government).

The council will issue solicited and unsolicited advice on relevant topics in the area of cybersecurity. Its recommendations have been underpinned, provide guidance, are strategic in nature and work at a practical level. Examples include the elaboration and implementation of strategic policy and research plans at government level, such as an International/National Cyber Security Strategy and the National Cyber Security Research Agenda.
The council is committed to providing practical advice and increasing awareness around cybersecurity. The members individually contribute to digital safety in the Netherlands by engaging businesses that deliver vital processes for our country in discussions at boardroom level. The aim during these discussions is to move cybersecurity further up the agenda. In order to achieve this, the council must ensure it is effectively positioned.

Re 2 Monitoring trends and new technological developments and, where necessary, translating these into potential measures to reduce the cybersecurity risks and to increase the economic opportunities.

The council makes preparations for the digital future by developing a vision on priority topics in the field of cybersecurity. Technological developments emerge at a breath-taking pace and new technologies are a significant driver of innovation and economic growth. The ability to identify and appraise technological developments and prioritise them in terms of their relevance will be key in this. The council will closely monitor trends and new technological developments and translate them into strategic recommendations as appropriate. Amongst other things, the recommendations will consider strategic measures that must be taken in order to mitigate cybersecurity risks and enhance economic opportunities.

Re 3 Initiating and/or accelerating relevant initiatives in the Netherlands and in the European Union that demonstrably contribute to raising the level of cybersecurity in the Netherlands.

The council may decide to launch or commission new initiatives. The CSR is able to use its position to request a specific organisation, government body or industry to implement a specific initiative. An example in this regard is the National Cybersecurity Summer School (NCS3). The council is able to issue targeted recommendations aimed at accelerating the strategic approach to cybersecurity. The global nature of cybersecurity means that the recommendations of the CSR will also address European and international avenues of approach.

1.5 Core values

The CSR operates according to the following core values:

Independence - The council is an independent body, which adopts a critical attitude towards all actors in the field of cybersecurity (countervailing power).

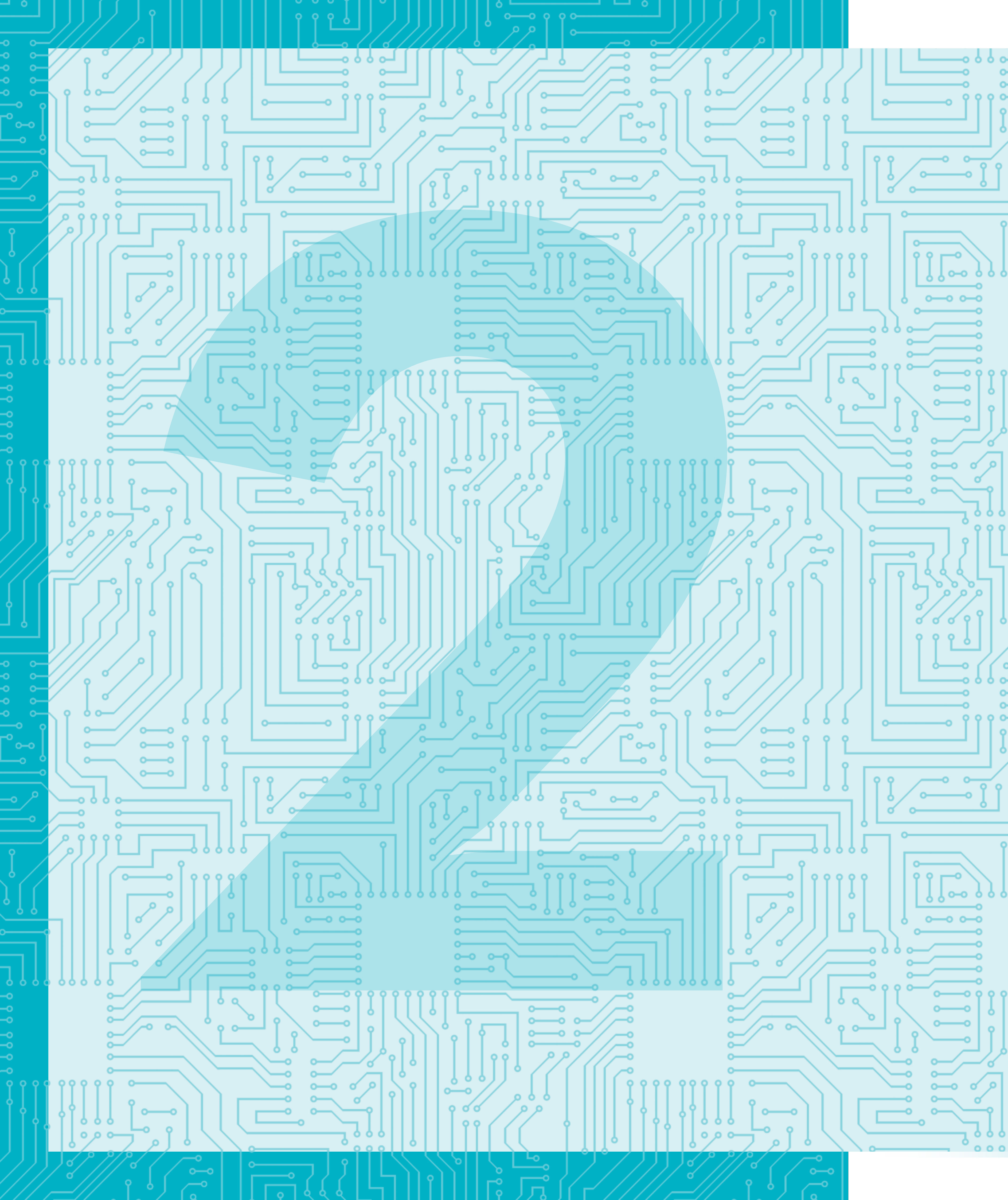
Common interest - The members will put the importance of security and prosperity in the Netherlands above their personal (business) interests and opinions. The power of collaboration with scientific, public and private organisations is used to full effect.

Forward-looking - The members will consider issues from a strategic and future-oriented perspective. The proposed solutions are partially inspired by a vision of the future.

1.6 Composition

The composition of the CSR is linked to the objectives set out in its work programme. The council aims for the widest possible representation of perspectives relating to cybersecurity. A total of eighteen seats are therefore taken up in a ratio of 7:7:4 – seven members from the private sector, seven members from the public sector and four members from the scientific community. The CSR has two co-chairs: one on behalf of the public sector and one on behalf of the private sector. The members represent organisations or industries relevant to the area of cybersecurity. Appointment of the members takes place in accordance with an established procedure.

The council's unique membership (drawn from public, private and scientific organisations) enables it to consider priorities, bottlenecks and opportunities against a wide range of perspectives. Our independence and critical attitude keep the Dutch approach towards cybersecurity finely tuned and in this way deliver a material contribution to a secure, open and prosperous society. The diversity of the CSR membership lends greater impact to its views.



KEY DEVELOPMENTS IN THE FIELD OF CYBERSECURITY

Recent times have seen the publication of various authoritative reports on cybersecurity, which consider the topic from a range of perspectives. The Cyber Security Council (CSR) has used a selection of these reports to prepare an inventory of key developments in the area of cybersecurity that will (continue to) play a role over the coming years. The publications were authored by well-established institutes and were the subject of reports in the Dutch media. This chapter offers a summary analysis.

2.1 Analysis of the reports

Overall, the Netherlands can be considered to be at the forefront of digitalisation. It is home to one of the largest internet hubs of the world and has superfast telecom networks for broadband. As a result, the Netherlands is currently ranked seventh in the world and fourth in Europe (2017) as regards 'e-government development and online service delivery'. This, however, is not to say that the Netherlands is fully cyber ready[1]. The objective of the Netherlands is to seize the opportunities that the new era will bring and maintain its digital position. The Netherlands must (continue to) function as a secure, open and prosperous society. A great deal of work remains to achieve this. Researchers have indicated that digital resilience in the Netherlands is lagging behind the growth of cyber threats.

Growing dependence on digital and other technologies

A key theme recurring in the reports is the fact that our society will increasingly come to rely on digitalisation. The use of digital technologies will continue to increase worldwide over the coming years, which could in turn lead to a greater dependence on IT. Over and above the year-on-year rise in the number of internet users, there is also a rapid global increase in the number of devices and appliances that are connected to the internet. As our dependence increases, so does the importance of cybersecurity. After all, our national and economic security are in part dependent on this. The public must be able to have confidence in society and social structures. Citizens and businesses must continue to be able to trust in the protection and the legal order offered by the government. The government must also look after those in society who are being left behind as a result of increasing digitalisation.

The Dutch digital infrastructure depends heavily on a select number of foreign organisations and this could potentially render the Netherlands vulnerable. Government bodies and businesses are increasingly seeking to exercise control over their own data. Within the European Union, a sense of urgency is gathering momentum around the need for safe storage of data and for control through a legal and regulatory regime in order to ensure compliance with European agreements.

[1] Potomac Institute for Policy Studies. (2017), The Netherlands cyber readiness at a glance, Arlington

Sovereignty

Sovereignty has been an issue of major significance within the digital domain for some time now. China and Iran are as yet (negative) examples of authoritarian states who use their sovereignty as a pre-text to close off a 'national' part of the internet. Western countries have in the meantime also begun to express opinions with regard to their sovereignty. This is predominantly in the context of better online and data protection, prompted in part by the revelations of Edward Snowden.

Analogue and other fall-back scenarios

As our society becomes more and more digitalised in the years ahead, our dependence is set to increase further. Dependence on digital technology carries great risks for the continued delivery of services, including those to society. This is because analogue fall-back scenarios are disappearing and alternatives will cease to be available. This drop-off can be attributed to a number of reasons, with the high costs of systems being cited as the main one.

Ethical and social challenges

Our growing dependence on digital technologies is giving rise to new ethical and social challenges. Public values and human rights such as privacy, equal treatment, autonomy and human dignity are threatened because the relevant legal frameworks, insofar as they currently exist, are not sufficiently forward-looking. Technological convergence means the frameworks from which we derive public values are no longer self-evident. As a result, the protection afforded to public values can currently be unclear and at times inadequate. Development of the frameworks will need to take place at European level as a minimum.

New technologies

New technologies represent both opportunities and risks. Research and innovation play a major role in developing solutions and can promote a safe application of (new) technologies. The Netherlands must (continue to) pursue this proactively, e.g. by developing knowledge and ensuring a timely response to any positive or negative impact that these technologies may have on our digital security, including with regard to ethical and public values. New technologies that will play a role in the years ahead include robotics, blockchain, biometrics, the Internet of Things (IoT), artificial intelligence, quantum computing and big data.

Supervision and guidance

Researchers have indicated that the Netherlands is currently lacking sufficient supervision and guidance in the area of cybersecurity. A secure, open and prosperous society requires coordination and guidance, both within government bodies themselves and in the context of public-private partnerships. The government must play a (leading) role in this regard, although its exact terms of reference have yet to be fully defined. There is also a high level of fragmentation, with many dissimilar parties being involved. As a result it is unclear which party has responsibility for what task. Responsibility for IT policy, and for cybersecurity policy in particular, is currently split among no less than five departments in our country and there are various agencies, autonomous administrative authorities and supervisory bodies that operate in this field.

Coordination of the various strategies and agendas is a pre-requisite for the development of an integrated approach[2].

[2] The Netherlands has developed various strategies and agendas in relation to cybersecurity. The Ministry of Justice and Security pursues National Cyber Security Strategy 2.0 - From awareness to capability; the Ministry for Economic Affairs and Climate Policy pursues Digital Agenda - Innovation, trust, acceleration; the Ministry of Foreign Affairs compiled International Cyber Strategy - Building digital bridges; the Ministry of Defence its Defence Cyber Strategy and the Netherlands Organisation for Scientific Research its National Cyber Security Research Agenda II.

(Public-private) partnerships

Public-private partnerships must also include cooperation with non-governmental organisations (NGOs). Examples of cooperation can be found within the critical infrastructure and the manner in which the Dutch banking sector tackles cybercrime. Nevertheless there appears to be scope for raising public-private partnerships to a higher level. In this regard, it is considered essential that these partnerships are strengthened and better coordinated. Such efforts should mainly centre on developing a culture in which the sharing of knowledge and experience and a better alignment of initiatives are felt as self-evident. Where cybersecurity is concerned, organisations must tighten cooperation with their chains.

The Netherlands should also continue to cooperate at international level. No single country can resolve the challenges around cybersecurity on its own, given their transnational character. The European Union is extending its statutory and regulatory regime, as evidenced by the NIS directive (Directive on security for network and information systems), the General Data Protection Regulation and the first draft version of the new European cybersecurity strategy published in September 2017. Within the EU, the Netherlands could play a strong role in shaping the agenda.

Investing in cybersecurity

Investment in cybersecurity must increase to ensure we are able to maintain our digital position and can continue to compete with countries such as the United Kingdom, France, Germany and the Scandinavian countries. Compared with competitor countries, where systematic investment is much higher, the Netherlands currently invests less than 0.01% of its gross domestic product (GBP) in cybersecurity.

Cybercrime

The Netherlands continues to be an attractive target for actors and it remains challenging to obtain insight into the extent of economic and other losses arising from cybercrime. Various organisations have carried out similar studies, which have indicated that there is no clear overview of the losses caused by cybercrime. According to recent estimates, the cost of cybercrime to Dutch organisations amounts to 10 billion each year[3]. The Netherlands has relatively high rates of cybercrime and cyber enabled crime. And yet the expectation is that in many countries cybercrime will surpass traditional areas of crime in scope in a number of years' time[4]. Even so, account must be taken of the fact that traditional areas of crime will evolve and take on a digital element.

In addition, National Security Profile (NVP) and the Cyber Security Assessment Netherlands (CSBN) have shown that the risk of cyber espionage by countries such as Russia and China is increasingly likely, exceeding that of epidemics, natural disasters and nuclear accidents.

Cyber terrorism and cyber sabotage are other significant risks that can lead to extensive economic losses and social disruption. Attention must be given to Industrial Automation & Control Systems (IACS) in order to prevent this. In the field of cybersecurity, the focus on IT is many times greater than that for operational technology (OT). A growing number of physical objects, including bridges, tunnels, locks and machines, are connected to the internet. Keeping these physical objects secure will be key to maintaining continuity and security in the Netherlands. The internet has yet to be recognised as a critical infrastructure in the Netherlands.

[3] Deloitte 'Cyber Value at Risk in The Netherlands', September 2017

[4] Internet organised crime threat assessment 2017, Europol

Attribution has been shown to be a difficult aspect of the fight against cybercrimes perpetrated by organised criminals or state actors. Actors employ technical options that make it difficult to trace the parties involved in a cyberattack. This means the perpetrators often escape prosecution, since it cannot always be discovered and/or established with certainty which type of actor was responsible for a specific cyberattack. One of the reasons behind this is the lack of (official) reports, resulting in an incomplete picture of cybercrime in the Netherlands. Insight into cybercrime is necessary in order to mount a more effective defence. The low reporting rate can in part be attributed to the complexity of the process involved in filing an official report. Another key reason for affected businesses not to file an official report is the possible reputational damage they might suffer.

The fight against cybercrime once again demands cooperation at European level since cybersecurity issues are transnational in nature.

Basic security

The level of awareness and the sense of urgency are still too low in our country. Government, citizens and the private sector are all taking steps to increase digital resilience, but this isn't happening fast enough. The human element in particular is proving to be a weak link in cybersecurity. We do not sufficiently acknowledge the opportunities and threats of digitalisation, nor have we embedded them in our thinking and behaviour. It is up to government bodies at all levels to lead by example. Citizens and the private sector must be able to transact safely online with the government. Information must be available online and data exchanges must be protected appropriately. Basic security must be up to par and networks must be protected against cyberattacks. Both the public and the private sector still have work to do to achieve an adequate basic level of security. A number of authoritative sets of standards and baselines[5] already exist in the area of cybersecurity and have contributed to good basic security. It is key this regard that suppliers adhere to the baseline and ensure clear communication in relation to the lifecycle of products and services.

Monitoring compliance with duties of care

Duties of care and product liability can act as incentives for manufacturers to look seriously at the digital security of their products. The American Federal Trade Commission (FTC) is one example of an active supervisory body in the field of IT. There is no comparable supervisory body in the Netherlands, which can take similar action against insufficiently secured IT equipment. The Dutch Data Protection Authority is responsible for monitoring and enforcing the data breach reporting obligation and ensuring the security of personal data.

In addition, current legislation imposes multiple duties of care on organisations in the field of digital security. There is a lack of agreement on what aspects ought to be covered under basic security. More attention needs to be paid to the enforcement of laws and regulations in the digital domain.

Cyberwarfare

Cyberwarfare is increasingly becoming a feature of political issues. An example is the significant interest in the digital influencing of democratic institutions in a number of Western countries, including the Netherlands. Influence on democratic values has become a significant risk. The Netherlands has added the cyber domain to its national security agenda, as has been done in other countries. Digital systems are an essential feature of all the fundamental interests that must be protected by the Dutch government. The cyber domain is increasingly becoming a target for geopolitical and terrorist threats. The Netherlands has begun to lay the foundations for cyber diplomacy. Work is also underway at the Organization for Security and Co-operation in Europe (OSCE) and the United Nations (UN) to develop global standards on cybersecurity. Greater transparency on permitted and prohibited actions and the remedies available in this regard will help to make conflicts more manageable in future.

Digital literacy

In terms of digital competence, the Netherlands is lagging behind several other countries. The Netherlands must safeguard its ability to continue functioning as a secure, open and prosperous society by making the development of digital competency in young people a structural feature of primary and secondary education. The aim is to better prepare them for the digital present and the future.

There has also to be a greater focus on cybersecurity and on career avenues in this field, in order to reduce the growing shortage of cybersecurity professionals.

[5] Examples: Baseline Informatiebeveiliging Rijksoverheid (Information Security Baseline for Central Government), Baseline Informatiebeveiliging Gemeenten (Information Security Baseline for Municipalities), Baseline Informatiebeveiliging Waterschappen (Information Security Baseline for Water Boards), the ISO27000 series and NEN7510. A Baseline Informatiebeveiliging Overheid (Information Security Baseline for Government Bodies) is currently being developed as a replacement for the existing government baselines.

2.2 Summary of trends

Growing dependence on digital and other technologies

- The use of digital technologies continues to increase worldwide and our dependence on IT grows in tandem with this.
- Both the number of internet users and the number of devices connected to the internet continue to grow.
- The Dutch digital infrastructure has been shown to be dependent on a select number of foreign organisations and this could potentially render the Netherlands vulnerable.
- The European wishes to ensure safe storage of data and cement this in a legal and regulatory regime.

Sovereignty

- Sovereignty is an issue of major significance within the digital domain.
- China and Iran are (negative) examples of nations using their sovereignty as a pre-text.
- Western countries too are putting forward opinions on their sovereignty. Their objective is better online and data protection.

Analogue and other fall-back scenarios

- The number of analogue and other fall-back scenarios is in decline in spite of our growing dependence on digital technologies.
- This carries great risks for the continued delivery of services, including those to society.
- The high costs of systems are the main reason behind this decline.

Social and ethical challenges

- Our growing dependence on digital technologies is giving rise to new ethical and social challenges.
- Public values and human rights are coming under threat because the relevant legal frameworks, insofar as they currently exist, are not sufficiently forward-looking.
- Development of new frameworks will need to take place at European level as a minimum.

New technologies

- New technologies represent both opportunities and risks.
- Research and innovation can promote a safe application of (new) technologies.
- The Netherlands must (continue to) pursue this proactively.
- New technologies that will play a role in the years ahead include robotics, blockchain, biometrics, the Internet of Things (IoT), artificial intelligence, quantum computing and big data.

Supervision and guidance

- The Netherlands is lacking in supervision and guidance in the area of cybersecurity.
- Coordination and guidance among government bodies and within public-private partnerships plays an important role.
- This is an area in which the government must lead, including by setting the example.
- There is also a high level of fragmentation, with many dissimilar parties being involved. As a result it is unclear which party has responsibility for what task.
- Coordination of the various strategies and agendas is a pre-requisite for an integrated approach.

(Public-private) partnerships

- Public-private partnerships must involve non-governmental organisations (NGOs) and must be raised to a higher level.
- Several good examples of this can be found within the critical infrastructure and the Dutch banking sector.
- Where cybersecurity is concerned, organisations must tighten cooperation with their chains by sharing knowledge and experience as well as coordinating initiatives.

Investing in cybersecurity

- The Netherlands must increase investment in cybersecurity to ensure it can continue to compete with the countries around it.
- Compared with competitor countries, where systematic investment is much higher, the Netherlands currently invests less than 0.01% of its gross domestic product (GBP) in cybersecurity.

Cybercrime

- Cybercrime will increase and surpass traditional crime.
- A recent estimate is that the cost of cybercrime to Dutch organisations amounts to 10 billion each year.
- The Netherlands has relatively high rates of cybercrime and cyber enabled crime.
- Cyber espionage by countries such as Russia and China is becoming an increasingly plausible risk, exceeding that of epidemics, natural disasters and nuclear accidents.
- Cyber terrorism and cyber sabotage also pose a significant risk in relation to cybersecurity.
- Attention must furthermore be given to Industrial Automation & Control Systems (IACS). In the field of cybersecurity, the focus on IT is many times greater than that for operational technology (OT).
- Attribution proves to be a difficult aspect, with perpetrators often escaping prosecution.
- One of the reasons behind this is the lack of (official) reports, resulting in an incomplete picture of cybercrime in the Netherlands.
- The low reporting rate can in part be attributed to the complexity of the process involved in filing an official report.
- Another key reason for affected businesses not to file an official report is the possible reputational damage they might suffer.
- The fight against cybercrime demands cooperation at European level.

Basic security

- The level of awareness and the sense of urgency remain too low in our country.
- The human element still proves to be a weak link in cybersecurity.
- It is up to government bodies at all levels to lead by example.
- Both the public and the private sector still have work to do to achieve an adequate basic level of security.
- A number of authoritative sets of standards and baselines have already been designed and are contributing to good basic security.

Monitoring compliance with duties of care

- More attention needs to be paid to the enforcement of laws and regulations in the digital domain.
- Current Dutch legislation imposes multiple duties of care in the field of digital security on organisations.
- The Dutch Data Protection Authority is responsible for monitoring and enforcing the data breach reporting obligation and ensuring the security of personal data.

Cyberwarfare

- Cyberwarfare is increasingly becoming a feature of political issues.
- Influence on democratic values has become a significant risk.
- Like other countries, the Netherlands has included the cyber domain in its national security agenda and begun to lay the foundations for cyber-diplomacy.
- Work is also underway at the Organization for Security and Co-operation in Europe (OSCE) and the United Nations (UN) to develop global standards on cybersecurity.
- Greater transparency on permitted and prohibited actions and the remedies available in this regard will render conflicts more manageable in future.

Digital literacy

- Children are the future. It is therefore desirable to ensure a greater structural focus in education on developing digital competency.
- There has to be a greater focus on cybersecurity and on career avenues in this field, in order to address the growing shortage of cybersecurity professionals.

2.3 List of references

The analysis provided in this chapter is based on a literature review encompassing the reports and publications listed below:

- Centraal Planbureau (2017), Cyber Security Risk Assessment for the Economy, The Hague;
- Gartner (2016), Special Report: Cyber security at the Speed of Digital Business, Stamford;
- Gartner (2017), Hype Cycle for Threat-Facing Technologies, 2017, Stamford;
- Kool, L., J. Timmer, L. Royakkers, & R. van Est (2017), Urgent Upgrade: protect public values in our digitalised society, The Hague, Rathenau Instituut;
- Munnichs, G., Kouw, M., & Kool, L. (2017), A never-ending race - On cyberthreats and strenghtening resilience, The Hague, Rathenau Instituut;
- National Coordinator for Security and Counterterrorism (2017), Cyber Security Assessment Netherlands 2017, The Hague, National Coordinator for Security and Counterterrorism;
- Potomac Institute for Policy Studies (2017), The Netherlands cyber readiness at a glance, Arlington;
- Verhagen, H. (2016), The economic and social need for more cybersecurity, Keeping "dry feet" in the digital era, The Hague;
- Scientific Council for Government Policy (2015), The public core of the Internet, The Hague/Amsterdam: Amsterdam University Press;
- Scientific Council for Government Policy (2017), Security in an interconnected world, The Hague: Scientific Council for Government Policy;
- World Economic Forum (2017), The Global Risks Report 2017, Geneva: World Economic Forum;
- World Economic Forum (2018), The Global Risks Report 2018, Geneva: World Economic Forum.

Photography: Jeroen de Bakker

CSR MULTIANNUAL STRATEGY

Clearly, the situation is urgent. As a nation, we have previously laid solid foundations that we can now build on, but we cannot become complacent. We must continue to increase the level of cybersecurity in order to maintain our leading position and be capable of seizing the opportunities offered in a secure digital economy. In this regard, it is essential that we identify strategic challenges and ensure a timely response to them. In line with its mission, vision and strategy, the Cyber Security Council (CSR) will continue to contribute to this in the years to come.

The preceding chapter provides an analysis that comprises an overview of key technological and other developments that will pose threats to a secure, open and prosperous society. From these developments, the CSR has distilled four strategic themes that the council will work on over the next four years, in order for our country to maintain its digital position and remain a frontrunner in the area of digitalisation. In this way, the council will help to strengthen cybersecurity in the Netherlands. The CSR will use the selected strategic themes to issue solicited and unsolicited advice on relevant topics in the area of cybersecurity to the government and, through the government, to private parties. And it goes without saying that the council will also continue to address topical issues that could arise in this complex area.

In addition to the multiannual strategy, the CSR will announce a two-year work programme which translates the strategic themes into concrete actions.

The strategic themes are as follows:

1. **Supervision and guidance**
2. **Growing dependence on digital and other technologies**
3. **Enforcement and monitoring**
4. **New technologies**

Re 1 Supervision and guidance

A secure, open and prosperous society requires coordination and guidance, both within government bodies themselves and in the context of public-private partnerships. The government must play a (leading) role in this regard, although its exact terms of reference have yet to be fully defined. As a result, coordination and guidance have remained limited.

Responsibility for IT policy, and for cybersecurity policy in particular, is split among no less than five departments. In addition to this, various agencies, autonomous administrative authorities and supervisory bodies are active in this field. There is no single point of contact (within the political structure). If we are to strengthen cybersecurity in the Netherlands, good coordination and guidance will be a pre-requisite. A first task must be the alignment of the various strategies and agendas, among which feature National Cyber Security Strategy 2.0 - From awareness to capability (Ministry of Justice and Security), Digital Agenda - Innovation, trust, acceleration (Ministry for Economic Affairs and Climate Policy), International Cyber Strategy - Building digital bridges (Ministry of Foreign Affairs), Defence Cyber Strategy (Ministry of Defence) and National Cyber Security Research Agenda II (Netherlands Organisation for Scientific Research). The CSR will act in an advisory capacity in this regard.

Re 2 Growing dependence on digital and other technologies

The use of digital technologies will continue to increase over the coming years, which in turn will increase our society's dependence on IT. The number of internet users is growing, as is the number of devices and appliances that are connected to the internet (Internet of Things). Industrial Automation & Control Systems (IACS) – systems used in vital and industrial sectors for the automatic control and monitoring of predominantly physical processes – represent another area receiving more and more attention.

This dependence on digital technology carries great risks, most of which arise from the increase in cybersecurity challenges. The growth of cloud services and the Internet of Things (IoT) increase the number of potential targets and, as a result, the level of risk. What is more, alternatives will (gradually) cease to be available. This could render the Netherlands vulnerable in terms of the continued delivery of services, including those to society, and this also threatens to impinge on our leading position in the area of cybersecurity.

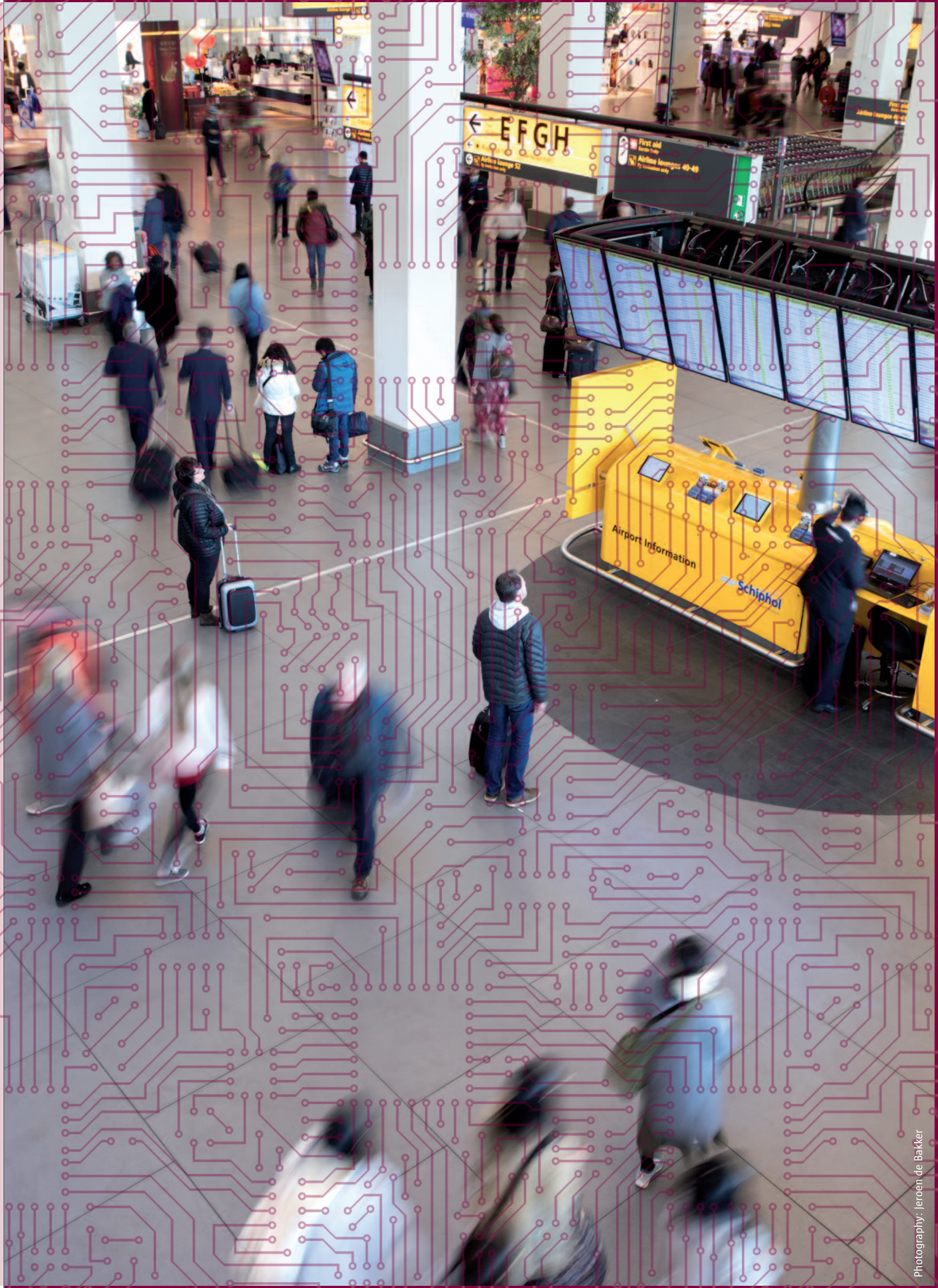
Re 3 Enforcement and monitoring

More attention needs to be paid to the enforcement of laws and regulations in the digital domain of our society. In contrast to other countries, there is no supervisory body in the Netherlands which can take action against issues such as insufficiently secured IT equipment. The Dutch Data Protection Authority has formal responsibility for monitoring and enforcing the data breach reporting obligation and ensuring the security of personal data. Certification for products and service could provide a solution in this area. If our country wishes to remain a frontrunner in the area of cybersecurity, monitoring and enforcement action must be carefully aligned with this.

The identification and prosecution of cybercriminals must be a priority and the shortfall in knowledge and personnel resources must be eliminated. It must also become much easier for citizens and businesses to report cybercrime.

Re 4 New technologies

New technological applications are emerging at breath-taking speed. Security-by-design and privacy-by-design should be starting principles for new technologies. However, many manufacturers are keen to rush their smart products to market. Their focus is to get there ahead of the rest, without first ensuring the digital safety of their products. This increases the importance of standardisation and certification. The council wishes to investigate the opportunities that new technologies can bring, ways in which opportunities can be converted into benefits and measures to cope with threats. One possible route to solutions is through research and innovation. The Netherlands must (continue to) pursue this proactively, e.g. by developing knowledge and ensuring a timely response to any negative or positive impact that these technologies may have on our digital security, including with regard to ethical and public values.



Photography: Jeroen de Bakker