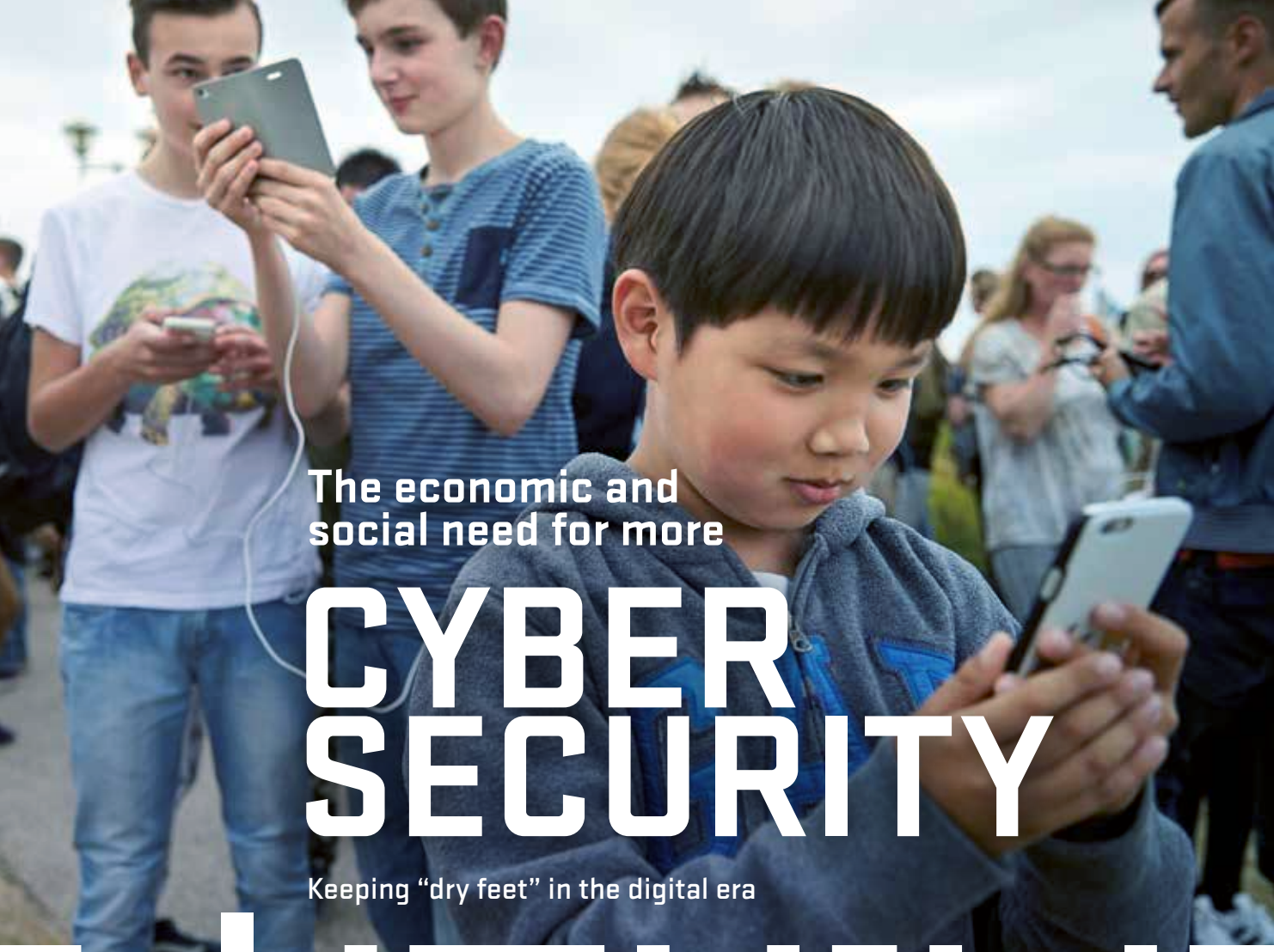

The economic and social need for more

CYBER SECURITY

Keeping “dry feet” in the digital era

Summary

Internet and ICT are now indispensable aspects of daily life. This is a global phenomenon, but is certainly true for the Netherlands. Our country is leading the way when it comes to digitisation. In almost all sectors of society digital technology is the most important means of processing and sending information or managing the primary business process.

New digital society and economy

The Netherlands has evolved to become one of the most ICT-intensive economies in Europe thanks to our first-class digital infrastructure. The Amsterdam Internet Exchange (AMS-IX), the world's largest Internet exchange, and our high-speed, broadband telecom networks, represent a large economic value plenty of good things our way. For this reason many large multinationals and IT firms choose for the Netherlands as their prime location to run their business from. E-commerce is generating new economic activities and job opportunities. Smart digital applications are contributing to innovation and progress in numerous sectors. Communication between citizens and government is increasingly digital in nature, and smart meters and equipment are becoming more common in people's households. Over the past 25 years, digital activities have made up in excess of one third of all economic growth. Over 5% of our GDP now comes from ICT. The digital economy now constitutes a third hub, together with Amsterdam Airport Schiphol and the Port of Rotterdam. A hub, moreover, that is growing more rapidly than other economic sectors.

Opportunities and vulnerability

Digitisation is therefore presenting huge opportunities for our 21st-century society and economy. This does, however, make it all the more important to ensure that the digital world is (and remains) safe and secure. Whether it is a matter of innovation, safeguarding sensitive company information, privacy or national security, cybersecurity is a prime requisite for a prosperous, safe society in the 21st century. Just as we protect our nation from flooding, we have to take effective defensive measures in the digital world. Only then we will protect ourselves from outside threats and be able to make the most of the opportunities that digitisation presents for the Netherlands.

Worrying increase in cyber threats

This is not obvious, given the increase in cyber threats. Vulnerabilities in ICT systems, such as inadequate security or outdated software, constitute the Achilles' heel of our digital security. Cybercrime now accounts for losses worth 10 billion euros in the Netherlands. The Cyber Security Beeld Nederland 2016 (CSBN 2016) paints a worrying picture of the security situation in the digital domain. Threats focus on theft of money and valuable intellectual property. Disrupting and sabotaging the services and processes of authorities and crucial social organisations is another target.[1] Large-scale societal destabilisation could ensue if, for example, power stations, transport systems or flood defences are attacked.

[1] Beleidsreactie op het Cyber Security Beeld Nederland 2016 (Policy Response to the Cybersecurity Landscape in the Netherlands 2016), Ministry of Security and Justice, 7 September 2016

Strengthening cybersecurity urgently

Consequently, there is an urgent need to strengthen cybersecurity in the Netherlands. The starting point for this will be increased attention: in Parliament, in the board room and at home. We all regard it as self-evident that there are rules, traffic lights and roundabouts for the purposes of road safety. And that companies supply safe, reliable equipment, food and drinking water to consumers. The security of the digital world should be equally important with the security and safety of the world around us. After all, criminal acts, espionage (including industrial espionage) and terrorism are just as much a threat online as they are out there 'on the street'. Citizens must be able to live safely and securely in a digital world, the business community must be able to do business properly, and the government must create the preconditions that enable these things. There is a lot to be done on all three fronts.

Governance and collaboration

Aside from cybersecurity and awareness, governance is a particular prerequisite if we are to safeguard our prosperity and well-being for the future. Governance t that unites government, politicians and private parties in a quest for the higher goal of creating a digitally secure living and working environment. The fact that cybersecurity, by definition, is also a phenomenon that transcends national and international borders is something universally acknowledged. Nevertheless, this advisory report focuses on improvements and actions that can be implemented in the Netherlands to bolster cybersecurity. Wherever relevant, reference is made to international or European discussion, legislation and initiatives.

The most crucial actions for more cybersecurity

This advice provides an analysis of the most significant threats and opportunities that digitisation presents for the Netherlands. Furthermore, it also contains concrete recommendations for actions in government, in the business community and in the home. To this end, cooperation between the public and private sectors is crucial. Bolstering cybersecurity and enhancing digital defence requires a programme of actions spanning several years along with an investment agenda. Such a programme should be drawn up by a Government in collaboration with the business community and local authorities. For the purposes of implementing this programme of actions, a top official who is directly accountable to the Government will need to be appointed. In addition, the government could set a good example by making security and privacy focal points in digital business operations.

Ensure stronger governance on the part of government:

- Unequivocal political control of the digital hub by way of an advisory council from the Ministerraad (Council of Ministers)
- Appointing a top official for the purposes of drawing up and implementing a cybersecurity programme of action spanning several years along with an investment agenda
- Getting our own digital infrastructure and business processes in order
- Modernising the authorisations held by the Dutch investigative, intelligence and security services, keeping checks & balances in mind
- Formulating future-proof legislation and regulations

Boost the private sector's own responsibility:

- Having the basics in order; satisfying the preconditions for cybersecurity
- Fulfilling duty of care in terms of cybersecurity
- Making chains more secure by introducing a chain responsibility
- Utilising an accreditation or certification system

Bolster cooperation between the private and public sectors:

- Intensify investigatory work on cyberattacks so as to ensure a swifter response and better prevention by expanding the Information Sharing and Analysis Centres (ISACs), the National Detection Network (NDN) and the National Response Network (NRN)
- Governance on public-private cooperation by high-ranking official and cybersecurity programme
- Ensuring advice by (evolved) Cyber Security Raad (CSR) that will have an impact
- Investing in cybersecurity according to the '10% criterion'

Make the Netherlands digitally skilled:

- Accelerated inclusion of digital literacy, including cybersecurity, in the core curriculum for primary and secondary education
- Encouraging development of cybersecurity knowledge
- Running targeted educational campaigns on cybersecurity for specific
- target groups (including SMEs) and the general public

Herna Verhagen
CEO PostNL