CSR MAGAZINE

Cyber Security Council

The economic and social need for more cyber security • Effective digital defenses are crucial • High-level government officials and business leaders speaking about cybersecurity in the Netherlands

Volume 3, Issue 1, March 2017

SPECIAL EDITION

CYBER SECURITY: EFFECTIVE DIGITAL DEFENCES ARE CRUCIAL

Foto: Niels Vos - Nationale Beeldbank

Hans Brinker: the boy who saves an entire village by plugging a hole in a dike with his finger – a Dutch legend invented by an American author in 1865. The Dutch fight against water is renowned the world over. Everyone realises how important it is. The government has invested in a Delta Plan to keep us secure. A vision, objectives, an action programme and a budget have been defined.

Hans Brinker: the hacker who saves the Netherlands by plugging a digital leak. This could easily be a Dutch legend as well, because our digital 'flood defences' are in serious need of attention. It is crucial that the level of cyber security in the Netherlands be improved, because we have one of the most ICT-intensive economies in Europe and we are therefore vulnerable to the ever increasing cyber threats.

When it comes to cyber security too, the Dutch government, in collaboration with the business community, must look to the future and deliver a vision, objectives, action programmes and funding. An ecosystem that keeps our country secure and exploits economic opportunities must be built through a public-private partnership. The independent report by Herna Verhagen, 'The economic and social imperative for more cyber security', endorses this view and gives guidance in this regard. Countries like Germany and the UK are investing heavily in cyber security. And they are not the only ones. The Netherlands cannot and must not be left behind. Thanks to our digital economy and society, the Netherlands can act as a role model in the field of cyber security. But, if this is to happen, we must invest. And we must work together. Politicians, the government, business and science must take action in partnership.

A high level of cyber security must be taken for granted, in the same way as high flood defences. In this magazine, senior government officials and business leaders give their views on how the level of cyber security in the Netherlands can be improved.

Eelco Blok, Dick Schoof, Cyber Security Council

CONTENTS


“Cyber security is the key to the success of our digital economy”
De economische noodzaak van meer
CYBER SECURITY

What is the economic and social imperative for more security? Herna Verhagen, CEO of the Dutch postal services company PostNL, was commissioned by the Cyber Security Council to produce an independent report on this issue. During the course of her research she spoke to a large number of cyber experts. "This produced interesting insights and good advice, around the opportunities too."

Herna Verhagen
CEO PostNL

EFFECTIVE DIGITAL DEFENSES

DIGITALISATION OFFERS HUGE OPPORTUNITIES

Verhagen handed the report and its associated recommendations to Prime Minister Mark Rutte and President of the Confederation of Netherlands Industry and Employers Hans de Boer at the Nieuwspoort press centre in October 2016 amid much public interest. This contributed to one of the Cyber Security Council (CSR)'s key objectives: to put cyber security at the top of the political agenda.

Why did you agree to the CSR's request?
"Cyber security affects everyone. The government and many large corporates have been working on it for some time now. And small businesses and individual consumers are also becoming increasingly aware of its importance. At the same time, cyber security is a fairly abstract concept and many people take the view that 'it's nothing to do with me'. Most people don't really understand cyber risks. Everybody's heard of phishing emails and a lot of people realise that not all websites can be trusted. It probably comes as no great surprise that consumers don't understand the risks clearly. But the same is true of many government authorities and businesses. Raising awareness of cyber risks and giving people advice on potential solutions is in the interests of the Dutch economy and Dutch businesses and authorities. I am delighted to have been able to use my position as CEO of PostNL to put this issue firmly on the agenda.
Personally, I don't just want to emphasise the risks, but also the opportunities. The Netherlands is leading the way in the field of digitalisation. We have the biggest Internet hub in the world, the Amsterdam Internet Exchange(AMS-IX), and a number of super-fast broadband networks. As a result, we have one of the most ICT-intensive economies in Europe. In 2015, more than 5% of our National Income came from ICT. Alongside Schiphol Airport and the Port of Rotterdam, our digital infrastructure forms the third mainport of our country. And that brings with it a wealth of growth and employment. The more effective our cyber security, the more we can reap the rewards that this brings."

Hans de Boer, President of the Confederation of Netherlands Industry and Employers:

“Cyber security is crucial for economic growth and prosperity. It must be addressed at all levels, by the government, by business and by consumers.”

When researching your report, you talked to experts on cyber security. What came to the fore in particular during these conversations?

“Unfortunately, what the cyber experts tell us is not very reassuring: the threats we are facing are extremely serious. Leaks, programming errors and poor security, for example, mean that many ICT systems are vulnerable. And, in addition, the government offers little in the way of coordination and guidance. There is not enough collaboration between government bodies themselves and between private and public players. Many different parties are involved with cyber security but it is not clear which party is responsible for what. Criminals are only too happy to take advantage of the limited governance and poor security of our digital world. Cyber espionage and cyber crime are commonplace. This picture is corroborated by a number of other academic reports and publications that we consulted on this issue. In the Netherlands alone, the damage caused by cyber crime and cyber espionage is estimated at an annual 10 billion euros, or around 1.5 percent of our GNP. Research also indicates that a significant proportion of this damage goes unnoticed. In a nutshell, this is a very worrying situation and we must take action to change it. The report contains clear advice and indicates specific measures that can be taken to improve cyber security. The initial priority is to focus more on cyber security: in the House of Representatives, in the boardroom and in the home.”

What are the key points of the advisory report?

“The recommendations relate to the role of the government, the role of the private sector, the collaboration between them and digital skills. One key piece of advice I would give the new government is: ensure that the digital 'mainport', or digital gateway, is given clear political guidance through a committee of the Council of Ministers and appoint a commissioner for cyber security. The job of this commissioner

Eelco Blok, Co-chairman of the Cyber Security Council:

“The competitive position of the Netherlands is under pressure. As, as a result, is our economy and our prosperity.”

Prime Minister Mark Rutte:

“It is good that this report recommends that digital skills form an integral part of the curriculum. If we make people cyberwise at an early age, we will reap the rewards in the long term.”

would be to devise and implement a long-term action programme with an investment agenda. The private sector must also get the basics in place and ensure that it meets all the requirements in terms of cyber security. And it must also make supply chains more secure by introducing supply chain responsibility. In the case of private service providers, an accreditation or certification system could be developed. Another action point is to make digital literacy, including cyber security, part of the core curriculum for primary and secondary education as soon as possible. It's also important to encourage the development of knowledge around cyber security. And, finally, we must all be prepared to invest in cyber security. The recommendation is that both the government and business set aside 10 percent of their annual IT budget specifically for cyber security measures. This benchmark is based on research around this type of investment in countries that are similar to the Netherlands. And, when buying a laptop, for example, consumers would be well advised to allocate 10 percent of the amount they spend to security."

Clearly there is still plenty of work to be done. What, in your view, should be the top priority?

"The most important thing is to put cyber security on the agenda. Following the publication of the report, there were many features in the media about the need for cyber security. The urgency of the matter is clear, and I hope and expect that the new government will build on this. And that both the government and multinationals, as well as SMEs and the Dutch people themselves, will realise that they all have a responsibility for cyber security. Everyone can do something. Greater awareness is a good thing, but what's needed now is action."

How do you see the future?

"We must take measures to improve our digital security and invest in it, that much is clear. And if we lead the way in this field, economic opportunities will result. As was the case with our knowledge and experience in the field of water management, for example. We have made a name for ourselves with our delta technology. We protect ourselves from flooding by putting up flood defenses. We can do the equivalent in the digital field by establishing effective digital defenses. If consumers and companies have confidence in a secure Internet, we can exploit the economic opportunities of digitalisation to the full."

"Invest 10% of your IT budget in cyber security"

"If we are to get to grips with cyber security, it is not only the government that must feel responsible for it but all parties in our society," says Director of the Rathenau Institute technology think tank, Melanie Peters. "The debate must focus not only on our security but also on other values such as health, equal treatment, access to essential goods and services, transparency, a fair price and ultimately our human dignity."

Dr Melanie Peters
Director of the Rathenau Institute

WE MUST HAVE A DEBATE AROUND THE BALANCE BETWEEN VALUES

CYBER SECURITY? IT'S NOT JUST ABOUT SECURITY

I got my first email account in 1993. At that time, I was working at the University of Texas, and we were some of the first to get such an account. The reason for this was that one of our lecturers, Dr Combs, had a particular interest in digital issues. Combs had drawn up some guidelines called "Safe surfing on the web". The cover showed a picture of a man in floral surf shorts standing in front of some very high waves. The message was: surfing is fun, but it's also dangerous.
Combs told us that the web had been developed for the army and that you never knew which route your messages would take. This was to ensure that the whole of the web wouldn't go down if one route failed. "Everything you write is screened, and you don't know where and by whom", he said. "If you send an email to a colleague wishing the president dead, you'll get a visit from the authorities."
Now, 24 years later, every time I send an email, I still think about the fact that someone can see it. But I'm well aware that my daughters and their friends don't think about this at all.
They have grown up with the Internet and see it as a fun thing that makes life easier.

Countless emails

I've been Director of the Rathenau Institute since 2015. The Institute is involved with research and dialogue around new developments in the field of science, technology and innovation. Its specific purpose is to inform politicians and the public and to give them the tools they need to make better decisions. In my work at the Rathenau Institute I send countless emails. I copy them to countless people, and forwarding emails is a breeze. I even receive emails in the evenings and at the weekend. Being without them for a couple of days would be unthinkable.
I've noticed that contact between colleagues and between organisations has become far less formal. And we send very few official letters.
The world has changed beyond recognition since the Internet left the world of amateurs 25 years ago and became something for us all. Toddlers get games from the web. An iPad has become a toy. My teenage daughter and her friends spend countless hours on their mobiles and order their clothes online (if they can get hold of their parents' ID).
The Internet and the applications associated with it are so easy to use that you don't have to

“Surfing is fun, but it’s also dangerous”

think about the world that lies behind them. That’s what makes it so appealing. But how can we do something about Internet security when we know so little about it? Or do we as users not need to get involved with it at all?

The Internet as a critical infrastructure

For a long time, the security of consumer products wasn’t seen as a problem. In any event, it wasn’t linked to cyber security. Until about five years ago when, for example, the Rathenau Institute published ‘You have been hacked!’, a magazine with the subtitle ‘cyber security can no longer be an afterthought’. The magazine was the result of an international project and listed studies carried out by partner institutes worldwide. It focused on the risks for critical infrastructures. In other words, infrastructures that are essential for the functioning of our society, such as the electricity grid, oil and gas pipelines, water pipelines or the transport system. But also hospitals and any other infrastructure that is necessary for health, safety, public order and economic prosperity. Even at that time, all these infrastructures were often controlled by digital means. And they were often controlled by networks that were leased from private parties and that were not subject to government protection and control. We warned people at the time that this would be the Achilles heel of these systems.

Cyber warfare

I can still remember one of the examples from the Rathenau report really clearly. It involved an Iranian nuclear power plant. In 2010, Stuxnet was discovered in a uranium plant in Iran. Stuxnet is software that spies on or subverts the types of computer that are used in industrial processes. Stuxnet was developed to attack the software on Siemens systems and was able to disrupt pumps, centrifuges and other components without being noticed. The capacity of the uranium plant dropped to 30%. It was assumed that only another country would be capable of producing such complex and targeted software and that the attack had therefore been masterminded by another country.
It comes as no surprise therefore that all the reports at the time focused on national action and international agreements to counter what was referred to even then as ‘cyber warfare’. If you could put a reprocessing plant out of action, you could equally well disrupt oil supplies or change the composition of drinking water, thereby damaging an entire country.

Small player, big damage

The World Economic Forum put the issue on the agenda, NATO was placed on alert and national governments commissioned research in the field. The UN was also urged to come up with initiatives in this regard. New international legislation and agreements in a WTO context were required, because these crimes go beyond borders, which makes detection and enforcement difficult. It was already clear at that time however that this critical infrastructure was vulnerable to attack not only by other countries but also by individuals or hackers operating in groups. A group called Anonymus sprang to mind. Small players they may be but it doesn't take them long to inflict big damage. To demonstrate this, TV journalists hacked a pumping station that protects the Netherlands from flooding.

The Internet of everything

But what if this critical infrastructure was also interwoven with consumer software? Because that’s what’s happening at the moment. Everything is connected to everything else. Take decentralised electricity supplies, for example. Energy from solar panels is returned to the grid whenever a household generates too much energy. Residents can monitor this using a smart meter, which is designed to be as user friendly as possible. How do you ensure that all the links in that network are secure? Is it enough to view the Internet and apps simply as useful tools? In my view, another example of critical infrastructure is false messages on Facebook. These messages can be circulated extremely easily and they influence public opinion and democracy. In the past, you couldn’t just change what was printed in the newspaper.
And it goes further than that. Not only do we use the Internet, the Internet also uses us. Not only do we read Facebook, Facebook also reads us. The electronic infrastructure collects data on us and combines it without us users even realizing.

Balance between values

In a nutshell, we can conclude that it’s not only the Internet that’s vulnerable and, as a result, our critical infrastructure and collective facilities. We as individuals are also vulnerable. And our dignity is vulnerable. Because nowadays cyber security also involves hacking or misusing personal data. Privacy and security are already high on the agenda but other values, such as our health, our autonomy, equal treatment and transparency, are not. In my view, the debate should be

about the balance between these values. When it comes to developments around new technologies and their impact on Dutch society, very few parties have a proper overview of the situation. And, as a result, we don’t have a proper understanding of the negative and positive opportunities for society either.
I’m not surprised that we don’t have a good overview of all the developments. On the one hand, the Internet was convenient and popular and we didn’t need to worry about it. On the other hand, there are major discussions around the 'cyber' topic that require international agreements. Now these two worlds are coming together. The problem of cyber security won’t be solved by citizens relinquishing their privacy and believing that the government alone will protect us.

Shaping society

The Netherlands is in a strong position. In many areas we are leading the way in ICT development. But we will only remain in this position if users become more cyber aware and social partners play a greater role. Take education, employers, software designers and companies that market apps and develop smart devices, for example. Cyber security isn’t just about security. It’s about the society that we want to shape together with the help of digital technology.

More information

- You have been hacked! Magazine produced by the Rathenau Instituut (2012) https://www.rathenau.nl/en/publication/volta02
- Big data and smart algorithms cyber security projects implemented by the Rathenau Institute https://www.rathenau.nl/nl/page/big data en slimme algoritmen

In recent years, the AIVD has focused increasingly on highlighting the dangers of using cyberspace. Clearly, the World Wide Web, smartphones and tablets are now an integral part of our everyday lives. We no longer find it unusual that everything in our homes and our transport systems is becoming ever smarter. But I wonder whether we are giving sufficient consideration to the risks.

Dhr. R.A.C. (Rob) Bertholee
Director-General of the General Intelligence and Security Service (AIVD)

ARE WE PAYING ENOUGH ATTENTION TO THE RISKS?

The increase in digitisation is not only leading to an increase in cyber crime. In my day to day work, I am also seeing a significant increase worldwide in cyber espionage and covert influencing on an almost indus trial scale. Clearly, this is only to be expected. Because with relatively little effort and relatively little expense, and a low risk factor, state actors can use the digital infrastructure to poke around to their hearts content in the economic, industrial, scientific and political files of other states. When you have more than a billion mouths to feed, stealing tried and tested agricultural technologies digitally rather than buying them or deve loping them yourself is worth the effort. If you believe that your country must acquire superpower status, reducing the influence of others by exer ting covert influence over them in public and political spheres using the Internet and social media is worth the effort.

Target of digital espionage
The Netherlands has an excellent digital infrastructure and both the public sector and the private sector are well equipped with all kinds of digitally controlled electronics. We also have some fairly valuable assets: aeronautical and space technology, agricultural innovations and a wide range of scientific knowledge, to name but a few. And the Netherlands is committed to and plays a significant role in Europe. All in all, the Nether lands is the land of plenty for malicious state actors. Government institutions and companies based in the Netherlands are an obvious tar get for cyber espionage. We are leading the way on digitisation but the level of protection we have implemented is not keeping pace with this.

Concerted effort
I am delighted therefore with Herna Verhagen s report. The report con firms our views and emphasises the urgent need to take significant measures in the field of cyber security. If we don t take these measures and if our security and earning capacity are undermined, the consequen ces and costs for our society will be enormous.

These measures can only be effective if they are taken in the context of a joint public private approach. This requires a concerted effort by govern ment, parliament, policymakers, administrators, regulators, companies and citizens. We all have a responsibility to protect our national digital security and, as a result, our economy, prosperity and society. As a public authority with significant digital ambitions, we must, in any event, make cyber security an integral part of our policies and activities.

Checks and balances
The unique tasks of the AIVD and the special powers that go with them enable us to make a significant contribution to cyber security. We are able to detect and analyze complex cyber attacks. And, as a result, we can offer high quality security advice to public and private bodies. And, where espionage or sabotage has been successful, we can offer high quality sup port with a view to limiting the damage. We are already doing this and we will continue to do so in the future. So, I believe that strengthening the National Detection Network (NDN) is a good start. Also, like Herna Verhagen, I am convinced of the need to modernise the powers of the AIVD and the MIVD (Military Intelligence and Security Service) under the new Intelligence and Security Services Act (Wiv). After all, the current Intelligence and Security Services Act dates from the era before the intro duction of the iPhone in Europe, so in some respects it is rather outdated. Having said that, I believe that also the checks and balances that apply to these powers must be brought up to date in a way that is workable in the long term. We are here for the Dutch people, not to keep some obscure regime in power. We are after all a secret service in a democracy.

Reducing the risks
The rapidly advancing digitisation brings with it significant opportunities. If we are to be able to exploit these effectively we must keep up to speed with the digital risks. We cannot feign ignorance on this. The AIVD will gladly assist in raising awareness in this regard and help reduce the risks.

“I am seeing a significant increase in cyber espionage and covert influencing”

Digital security and security through digital solutions. In my view, that must be the core of future security policy. We must invest to promote the desired developments in society but also to prevent the widespread disruption to society that may ensue. As Herna Verhagen's report 'The economic and social imperative for more cyber security' makes clear, this is not happening nearly enough. Things are moving very quickly. Urgent action by the government is therefore crucial.

Wim Kuijken
Chairman of the Board of
The Hague Security Delta

NEW GOVERNMENT MUST INVEST HEAVILY IN CYBER SECURITY

"Together with territorial security (Defense), social safety (Police, Fire Services) and physical safety (delta plans), cyber security is the issue of the future."

Together with territorial security (Defense), social safety (Police, Fire Services) and physical safety (delta plans), cyber security is the issue of the future. As in the physical world, we must not wait for a flood to happen before we take action. Cyber crime has the potential to cause serious disruption to our society. Our critical infrastructures, e.g. our mobile networks or our energy grids, could be jeopardised by attacks by criminals or even other countries. We must therefore protect these critical infrastructures more effectively and, ultimately, the government is responsible for this. It would be great if we could, so to speak, raise the digital drawbridge in the Netherlands in the event of an incident. But this will require better insights and more powers. The sooner we take these measures, the more attractive the Netherlands will be as a base for businesses and institutions. And people will also have confidence in the government when it comes to security.

Invest in advance

Cyber security must be tackled innovatively through a public-private partnership, ideally in the form of a network. The government must be a key driver here. In the field of (digital) security in particular, it must invest in innovations and act as an early adopter. This public-private partnership approach must however be implemented under the auspices of the National Coordinator for Security and Counterterrorism and with the necessary resources for development and application of the National Cyber Fund. My advice is to invest in advance and reap the many rewards that this will bring: making and keeping digital applications secure, improving the protection of digital networks and critical infrastructures on a long-term basis, stimulating economic growth and building trust.

Dependence on ICT

Dutch society and the Dutch economy are becoming ever more digitalised and, as a result,

ever more dependent on ICT. There's no stopping the Internet of Things. We are no longer just using the Internet for online news and shopping, we are also banking online and increasingly the systems we use to heat our homes are connected to the Internet via our mobile phones. What's more, in the not too distant future, we may also be riding around in autonomous cars and receiving parcels delivered by unmanned drones. And it's not only our homes and devices that are connected to the Internet through all manner of sensors. The same applies, for example, to our living environment, where traffic lights in 'smart cities' are interconnected. And the industrial automation systems of our critical infrastructures in the fields of water, energy, telecommunications and healthcare, amongst others, are also fully digitalised. This trend brings with it much potential and many new economic opportunities but it is not without its risks. Particularly since it involves the most crucial parts of our society. So we don't have a choice: the cyber security of our critical infrastructures must be improved. And, if this is to happen, more money will have to be invested.

Unique digital infrastructure

The Netherlands is ideally positioned to exploit the trends of digitalisation, the Internet of Things and 3D printing as part of the so-called fourth industrial revolution: we have a unique digital infrastructure that we can use as a base and, with the two biggest Internet hubs in Europe, we are also a global center for data traffic. This makes the Netherlands attractive to international businesses and organisations and provides a wealth of economic opportunities for the IT and security sector.

"We don't have a choice: the cyber security of our critical infrastructures must be improved."

“Dutch society and the Dutch economy are becoming ever more digitalised and, as a result, ever more dependent on ICT.”

National Cyber Plan

If we are to have a successful society and economy, we must ensure that our digital critical infrastructures are neutral and secure. We must therefore develop a national approach to cyber security to protect our physical critical infrastructures, just like the Delta Plan. And because no single organisation is responsible for cyber security of the Netherlands, this must be implemented both on the basis of constitutional principles and through a public-private partnership. It must be tackled in an integrated way by both the government and businesses. An approach that will only work if it is based on a long-term national investment programme, which is included in a National Cyber Plan.

National Cyber Testbed

We have already made a start on this within the national security cluster The Hague Security Delta, in which businesses, governments and knowledge institutions collaborate on innovative solutions in the field of IT security. So, for example, together with our partners, we are looking at how we can set up a National Cyber Testbed for critical infrastructures. This would be the first cyber test and development center of its kind in Europe, and would allow among others data center, telecommunications companies and energy suppliers to test the cyber security of their systems, trial innovative security solutions and deliver training in a protected environment.

I also see a role for the testbed around the development of The Internet of Things and Smart Cities. We must make it so that products such as smart thermostats, traffic lights and locks are not launched on the market until their cyber security has been tested and they have been awarded a certification mark, just as we did with the KEMA certification mark following the introduction of electricity. Only by tackling cyber security in a similar way can we prevent serious cyber disruptions.

The establishment of a testbed of this nature will require close cooperation between the critical infrastructures sectors and millions of Euros of investment. This is crucial for if we are to keep our society secure and be in a position to exploit the economic potential of our ICT and cyber security sector and market our knowledge on international scale.

Finally

In a nutshell, the more digitalised our society becomes, the more cyber security is the only answer to the problems that this new world entails. So, we must focus on a combination of exploiting the economic opportunities on the one hand and managing the risks on the other. A National Cyber Plan, including an investment programme, is essential in this context. That way, we will provide Dutch businesses with the firm foundation that it requires, and the Netherlands can rightly position itself as a secure digital gateway to Europe.

The Netherlands is not a small country. Our economy and our IT sector are world leading, our knowledge of IT and our IT infrastructure are first rate, and we also regularly feature at the top of other rankings. We must not underestimate our abilities. We are in a good position and we can be a world leader in the fight against cyber crime and in the development of systems that improve the level of cyber security. But if we are to exploit the huge economic opportunities that are available to us, we must raise our self-confidence.

Paul de Krom
Chairman of the Executive Board
Chief Executive Officer of the
Netherlands Organization for
Applied Scientific Research (TNO)

DON'T LET OUR COUNTRY BE PLUNDERED!

EXPLOIT THE ECONOMIC OPPORTUNITIES

The leading position we are in now is due to investments we made in the past. But we are currently in danger of missing the boat. According to the Harvard Business Review, the Netherlands is in the "rapidly receding" category. Other countries are investing more and are making faster progress. If the Netherlands doesn't take action to rectify this situation, things will get worse and security will not keep pace with cyber threats. We are in danger of bringing up the rear internationally, although this need not be the case.

Recommendation 1: develop a vision
If we are to lead the way in this field, the first thing I would recommend is that the Netherlands develop a cross-governmental vision and significant ambitions in the field of cyber security. Only then can we exploit the economic opportunities that are available to us. At the moment, we are working in a very fragmented way. For example, it's not clear to me what role the three main players (the Ministries of Defense, Security and Justice, and Economic Affairs) play in this context. In any event, the importance of cyber security to the Netherlands is too great and the Netherlands is too small to waste time on all manner of 'bureaucratic nonsense'. There is also a lack of investment, momentum and focus. The role of the government as a champion of the public interest, in ensuring maximum security and as an investor and early adopter is crucial. If we are to tackle the cyber security issues that we are facing, protect the Netherlands and exploit the economic opportunities that cyber security brings with it, we must work together and make the Netherlands stronger.

Recommendation 2: make ourselves resilient
The national vision and ambition around cyber security must also address ways of making our country resilient. At the moment, we are not devoting sufficient attention to this. It's easy to prepare for the expected, but what we are dealing with here is the unexpected. We must be able to manage this too. My second recommendation therefore is this: develop scenarios. What should you do in the event of an unexpected cyber (security) developments? How do you protect yourself from cyber attacks? There's no such thing as 100% security but you can minimise the risks. We also need scenarios that help us achieve the position of world leader and to take action if things don't go according to plan. That way, the Netherlands will be resilient on two fronts.

"We are in danger of bringing up the rear internationally, and this need not be the case."

Recommendation 3: take control

In essence, the cyber security structure in the Netherlands is good. We have the National Cyber Security Centre as an operational unit, the Cyber Security directorate as a policy department (both come under the Ministry of Security and Justice) and the Cyber Security Council as an independent consultation body. It's an excellent, layered approach that takes the form of a public-private partnership. And we're good at that – far better than other countries. Some countries have tried to copy our model but they have not succeeded. It's simply in the Dutch DNA. Only in this way can we achieve the momentum and focus we need to tackle threats quickly and efficiently and to take advantage of the economic opportunities that are available to us. We must use the structure that we have to press ahead quickly. We need a shared, long-term knowledge and investment agenda, in which government departments, business, knowledge institutions and science work closely together. My third recommendation is to appoint a senior-level official or minister to organise, control and coordinate this process who would report to a steering group in the Cabinet, advised by the Cyber Security Council. This council must monitor the national vision and ambition and offer advice to all the parties involved.

Recommendation 4: share knowledge

Here in the Netherlands we must focus more on technology and product development. Many products currently come from the US and Israel, but they should also come from the Netherlands. A huge amount of knowledge is available but it is not being properly exploited. We acquire one piece of knowledge after another without the government, businesses and academic institutions sharing this knowledge effectively and translating it into security products that can be launched on the market. This must change. My fourth recommendation is therefore to make it easier to share knowledge between the government, businesses and the sciences. It must also be clearer who is in possession of what knowledge, so we don't have to reinvent the wheel. It must be possible to share information about cyber attacks and breaches, for example, anonymously. Sharing knowledge will make the Netherlands more secure and will enable us to develop exceptional security products that are in demand the world over on account of their efficiency and reliability.

Recommendation 5: invest

What a waste if good ideas for cyber security products die an early death because they don't progress from proof-of-concept to an actual product. This is a well-known phenomenon that is known as the 'valley of death', which makes people loath to make risky investments. It happens, for example, if the return on investment is too uncertain for businesses. They cannot bear this burden alone. I therefore recommend that sufficient risk capital be made available, so that this 'valley of death' can be overcome. In this phase, government funding is crucial. This will act as a multiplier, because businesses will then invest. This will result in secure Dutch products that we can trust, with the Dutch government acting as an early adopter.

"The Netherlands must develop a cross-governmental vision and significant ambitions"

Photo: Aerovista Luchtfotografie - National Photo Bank

There's no such thing as 100% security but you can minimise the risks. Make the Netherlands cyber resilient.

Recommendation 6: create an ecosystem

In my view, we must create a cyber ecosystem in the Netherlands of which universities, knowledge institutions, the government and business must all be part. An ecosystem of this type would provide insights into each other's knowledge and this knowledge could then be confidentially and easily shared with a view to developing products that could be brought to market. Knowledge would be shared on an ongoing basis and there would be ongoing collaboration over cyber security products, in response to current trends. An ecosystem involves co-creation, the courage to try things out, the taking of risks, because innovations aren't always successful, and the will to work together, to make the Netherlands more secure and to exploit economic opportunities.
A programme that facilitates this ecosystem must be put in place.

And finally...

Cyber espionage is a major challenge. We must prevent ideas, innovations and blueprints for products disappearing abroad. Equally, when you import products from abroad, you don't know exactly what and who you are bringing in. Dutch products enhance our security. We must not let our country be plundered. The national interest is too great for that.

"Launch a programme to facilitate the cyber ecosystem"

Hans de Boer
President of the Confederation of Netherlands Industry and Employers (VNO-NCW)

In my view, cyber security is crucial if we are to be in a position to exploit the opportunities that digitalisation brings and to maintain people's trust in it. As we have seen in recent months, cyber warfare is cheap and effective. This calls for first-rate security. Otherwise parts of our society may soon be immobilised in a way that we have not seen before.

CYBER WARFARE IS CHEAP AND EFFECTIVE

DOING NOTHING IS NOT AN OPTION

Critical infrastructures such as energy, water and telecommunications are the first thing that comes to mind when I think of vulnerable sectors where cyber attacks could have a major impact. Remember how much damage a broken lock gate caused recently to businesses and the public. That was a physical accident. A conventional accident, but it could just as easily have been a cyber attack.

Maintain trust

At the same time, cyber security is crucial for society as a whole. Our dependence on IT is increasing by the day. We can no longer do without it. We shop, order, pay, chat and date online. More and more business processes are fully or partially automated. Everything from payments to logistics, and from production processes to customer files. Information technology brings with it unprecedented new opportunities, but our dependence on ICT also has a downside. It makes us vulnerable to abuse and failure. Cyber crime is already costing our economy billions of euros. In my view, cyber security is crucial if we are to be in a position to exploit the opportunities that digitalisation

brings and to maintain people's trust in it. It is therefore a key part of our Next level programme, which is directed at the new government.

Solutions

Although the whole saga with the Democratic Party in the US is clearly bizarre, hopefully it has significantly raised awareness. Whether it be amongst the business community, political parties or citizens and NGOs. In my view, the main solutions will be found in three areas:

- More awareness.
  This is already happening, but this greater awareness must lead to action!
- More collaboration.
  Between businesses and the government but also cross-border collaboration, for example. Because many of the cyber threats are international in nature and require international solutions. I'm thinking here, for example, not only of the sharing of information on cyber threats and the development of standards but also the detection and prosecution of cyber criminals.
- More resources.

Everyone must play their part

Ms Verhagen's report is an excellent document that makes it clear exactly where action is needed. Both the government and businesses, large and small, must play their part. Doing nothing is not an option. We must also ensure that cyber security remains high on our members' agenda. Small businesses, for example, are quite often unaware of the cyber threats they are facing. That's why we are focusing on this area in particular.

International approach

A trend that is becoming increasingly common and that is advancing rapidly is what is called the Internet of Things. All kinds of devices are connected to the Internet. Whether it be a thermostat, a smart refrigerator, a car or medical equipment, billions of devices are now connected and their number is increasing by the day. Clearly, these devices must be secure. A moving vehicle or medical equipment being hacked is unthinkable. Let one thing be clear: The Internet of Things offers us major opportunities but if we are to retain people's trust in its security we must take the security risks seriously. An international approach is the obvious way forward in this context.

First-rate security

Things are moving so fast and, given the strong growth that we have achieved in digital services over the past fifteen years, we are relatively vulnerable. I was recently in Belgium where the government is still relatively un-digitalised. That is not the case in the Netherlands. Take the example of the lock gate that I just mentioned. This wasn't a cyber incident but such cyber risks exist. In the Ukraine, there have been incidents of power stations being shut down. We must make ourselves resilient to this. As we have seen in recent months, cyber warfare is cheap and effective. This calls for first-rate security. Otherwise parts of our society may soon be immobilised in a way that we have not seen before. And that's to say nothing of the impact of fake news, 'cyber influencing' in political spheres etc.

New government

I expect the new government to provide three things: resources, measures and customisation. Action is required on all three fronts and this can't happen without additional resources. Customisation and targeted actions are required not only to protect our critical infrastructure but also in other parts of our economy. Companies in the top sectors, which are crucial to the earning capacity of our economy, appear, for example, to be extremely vulnerable to cyber espionage.
An effective approach also requires targeted investments by the government. A few months ago we presented our vision of the future and related investment agenda 'De digitale kwantumsprong' (The digital quantum leap). As it should do, cyber security plays a key role in this and we are calling on the government to invest 100 million euros in cyber resilience.

Digital trust centre

Amongst other things, we are calling for the establishment of a digital trust centre, a knowledge centre that businesses can use to report threats, ask questions and obtain advice. In my view, cyber issues can only be tackled effectively if there is intensive collaboration between the public and private sectors. The government and business depend on each other to improve our resilience to cyber threats and to devise solutions. I also see cyber security as a real opportunity for the Dutch cyber security industry. We would very much like to see the government stimulating the national market for cyber solutions.

Clear guidance

I am confident about the future. We are already making significant progress. I believe that our small size, strong government and strong businesses will enable the Netherlands to tackle this problem successfully. We are already exporting this knowledge and hopefully we will be doing so even more in the future. But we must work together: government, businesses and social partners. And it's also important that there is clear guidance on cyber security across the various government departments. A well-coordinated, joint approach is crucial. Including digital literacy in the curriculum is also a key issue for us. Children must learn to deal with digital issues and be aware of the risks from an early age.

"Cyber crime is already costing our economy billions of euros"

Photo: Frank Noordenbos - National Photo Bank

Customisation and targeted actions are required not only to protect our critical infrastructure but also in other parts of our economy. Companies in the top sectors, which are crucial to the earning capacity of our economy, appear, for example, to be extremely vulnerable to cyber espionage.

Bas Eenhoorn
National Commissioner for Digital Government (Digi-commissioner)

BUSINESSES AND GOVERNMENT MUST HAVE A GREATER SENSE OF URGENCY

Robespierre, freedom fighter and tyrant during the French Revolution, tellingly described the delicate balance between transparency and ignorance as follows: "The secret of freedom lies in educating people, whereas the secret of tyranny is in keeping them ignorant". Almost 250 years later, in the era of the fourth revolution (of the digital kind, this time), his words are still just as poignant.

In an age in which technological developments are increasing exponentially, to the extent that it is sometimes difficult to take them all in, it is still important to keep up to speed and to take a critical perspective on what's going on. Robespierre's views on education and ignorance still fascinate me. On the one hand, I want to know how artificial intelligence and big data can help me and what I can do with it. On the other hand, I have the sense that the companies that play a leading role in this are keeping me ignorant.

Losing trust

Major tech companies from Silicon Valley are leading the way in the development of artificial intelligence and the use of big data. They are applying the opportunities that these developments offer in their services. As a result, people are becoming 'dependent' on their free services. Free: after you accept the terms and conditions of use, which, like I suspect every other consumer, I don't read before I accept. Ignorant of what I have agreed to, I set to work, having surrendered a significant part of my privacy to the tech giants. Following reports of security leaks, hacks, spyware and malware, I am rapidly losing the trust I had in these companies to protect my data effectively and use it wisely. Moreover, the growing realisation that the code behind their services (the algorithms) can no longer be understood or verified by humans just makes things worse. It means that no one knows whether he or she is receiving all the relevant information and whether the news that is being reported is actually genuine. The complexity and pace of developments confirm my view that concerted action by government and citizens is required if a healthy balance is to be restored.

Netherlands will lead the way

When it comes to interpreting and applying new developments, politicians, policymakers and the government, business and science must work more closely together. This will allow us to exploit the opportunities that these new technologies offer us and will enable the Netherlands to lead the way in the fourth revolution. It is important that people are digitally literate and are given any support they may require in this regard. Educators and the education system play a key role in making children more digitally literate and cyber wise.

Urgent action is required

I'll leave you to decide whether Robespierre was a tyrant or a freedom fighter. What I do know however is that exponential technological developments don't leave much time for endless reflection and that urgent action is required. That's why I embrace the conclusions of the Verhagen report and see investment in cyber security as a prerequisite for secure digital services. My challenge is to increase the sense of urgency of business and the new government. I will also focus on improving collaboration between business, science and government. Only in an ecosystem that focuses on a common interest and common goals, can we effectively deploy our increasingly scarce resources and make the best possible use of the opportunities that this new technology brings.

"Algorithms can no longer be understood or verified by humans"

One morning a few years ago, Shell employees came into work and found, to their amazement, that they were unable to utilise the company's ICT services. Applications could no longer be used or generated strange error messages, files could not be opened and connected systems waited endlessly for responses.

Marjan van Loon
President Director of
Shell Nederland

FURTHER DIGITALISATION MAKES THE NEED FOR CYBER SECURITY EVEN GREATER

A SCRIPT DEACTIVATED ALL THE SERVERS IN MALAYSIA

The problem was caused by a data center in Malaysia where hundreds of servers were suddenly and unexpectedly deactivated and, as a result, thousands of Shell employees all over the world were unable to do their work.

Disruption with a huge impact

Shell's own IT organisation and our IT suppliers quickly became aware of this major disruption. All efforts were focused on getting the application servers back online. Ultimately this recovery process took weeks, resulted in thousands of hours of lost production and eventually had a huge financial impact. It was soon clear that the problem had not been caused by a technical defect: a script that had systematically endeavored to sabotage all the servers in the data center in Malaysia was discovered.

Industrial Control Systems

I wish I could say that this was the last such incident at Shell. Unfortunately, however, that is not the case. Cyber incidents take place on a regular basis, although luckily they're not always on the same scale as the incident in Malaysia. These cyber incidents make it painfully clear how dependent major organisations like Shell have become on their ICT services. And it's not only support departments within Shell that are dependent on IT, Industrial Control Systems for oil and gas extraction, and the refining and distribution of semi-finished and finished products also play a key role in our processes. These systems must be properly protected against cyber threats.

Cyber security is a key priority

Here at Shell we try to simplify, streamline and digitalise our business processes on a daily basis. Shell has defined an IT strategy for this purpose, which means that Market Standard services are used for the majority of existing and new ICT services. In a nutshell, this strategy ('Market Standard, unless') means that the majority of our data is no longer stored in Shell- managed data centers but is distributed in various Software-as-a-Service (SaaS) solutions.
And Shell employees are increasingly able to perform business processes more efficiently with the help of digitalisation.

As a result, Shell's IT footprint will change significantly over the next few years. Clearly, the protection of our data – our Intellectual Property and Competitive Sensitive Information – must not be jeopardised through the implementation


“Create a secure platform so information can be shared on a sector basis”

“Directors are regularly informed about new cyber security threats”

of this strategy. This requires a different approach to cyber security and skills that are consistent with this. We must ensure that only authorised users gain access to our data, and that if security incidents in our IT systems are reported, we as an organisation are equipped to respond adequately to them. Consequently, cyber security is and will remain a priority for Shell.

On the boardroom agenda

One can’t work effectively and securely without cyber security. Shell has an Information Risk Management (IRM) department that focuses on risk management, monitors critical IT systems and coordinates cyber security processes. IRM is also responsible for making Shell’s employees aware of ICT risks within their business processes. In addition, end users’ awareness of cyber security is raised through campaigns. Cyber security is also high on the agenda of the Board: directors are regularly informed about new cyber security threats, security incidents that have taken place or significant IT or information risks that could disrupt our business processes.

More integrated cyber legislation

I found Herna Verhagen’s report on cyber security an extremely interesting read, and it confirms to me that Shell is doing the right thing by taking information security so seriously. Here at Shell we’ve already been working on many of her recommendations for some time. But the report also makes new recommendations that we will evaluate further internally.
Certain aspects of the report interest me in particular, such as more cyber security legislation at European level. For a multinational like Shell, which has operations in more than 70 countries, complying with national IT legislation is a complex and time-consuming process. If we release a mobile app, for example, we have to establish for each country individually whether the app and the collection of personal data complies with the regulations in that country. More integrated cyber legislation at European or ideally even global level would allow international organisations to operate more effectively.

Platform for sharing information

The sharing of information between public/private organisations around current cyber threats against vital infrastructure, for example, is also a recommendation that we support. Cyber criminals are generally well organised and operate in professional groups to attack governments, businesses or critical infrastructure such as power stations, water treatment works and gas distribution networks. Sharing detected attacks, under embargo or otherwise, could help both the government and businesses prepare themselves better for such incidents. As stated in the report, the government must take the lead on this by creating a secure platform on which relevant information can be shared on a sector basis.

Invest in education

Finally, whether it be the US presidential elections, the power grid in Ukraine, the huge number of Yahoo! accounts that were hacked or the compromised IT of government services, cyber threats are playing an ever more prominent role in our lives and we must defend ourselves adequately against them. Investing in specialist expertise in the field of cyber security in secondary and higher education is crucial in this context. This aspect features in the report but, in my opinion, it should be higher on the government’s agenda.

People often see cyber attacks as remote events that are nothing to do with them. But nothing could be further from the truth. Not so long ago RTL News demonstrated just how easy it is to take over the twitter accounts of members of the House of Representatives. This may seem a bit trivial but hackers use the same method of attack to penetrate systems.
They then steal important information, disseminate false information or lock the hard drive using ransomware. Or they sabotage systems in vital sectors on which we as a society depend, such as our energy or water supplies. Let these examples and everything we see and hear in the news about cyber crime and cyber attacks serve as a wake up call to us. We can t just ignore things and act as if there is no risk. We are seeing a growing and real threat from professional criminals and foreign intelligence services and it is crucial that our defenses keep pace with this.

Cyber conscience

In my view, there are parallels to be drawn between the offline world and the digital world. The government won t come and put a lock on your front door, and a civil servant certainly won t come and lock it for you every evening. So you can t expect the government to do so in the digital world either. For example, you yourself are responsible for the safe use of your passwords. That is the principle on which everyone must work. And I see another parallel with the partnerships that have been established between the government, business and science in the offline world to keep the Netherlands safe. The government can t do this on its own. The same is true in the digital world. The vast majority of the digital infrastructure in our country is in private hands. So, if we want to achieve our objectives, it s crucial that we work closely together. In this context, I think it s fantastic that we have the Cyber Security Council (CSR), in which both these sectors are represented. The Council looks strategically at the opportunities and threats of new technological developments from a number of different perspectives, and this role is becoming ever more important. In my view, the CSR must act far more as a cyber conscience for government, business and science.

Safe place to do cyber business

This partnership between the public and private sectors and science is unique and is ideally suited to the Netherlands. Even the hacking community is involved. We are used to compromise, to consulting with each other in order to achieve a joint result. One example of this is the National Cyber Security Centre (NCSC), which comes under the National Coordinator for Security and Counterterrorism (NCTV). Here public and private partners work together side by side to keep the Netherlands cyber secure. Not many other countries can say the same, so, in my view, we are still leading the way in this field. As a result, other countries regularly ask us for advice. A great deal of progress has been made through the action programme of the second National Cyber Security Strategy, which promotes the procurement of secure software. And public campaigns such as Alert Online raise awareness. We are also investing in innovation and education, with the setting up of the Dcypher knowledge platform, for example. In addition, during its presidency of the EU, the Netherlands took the opportunity to put cyber security firmly on the international agenda.

Internationally, the Netherlands is leading the way on digitalisation and, in recent years, has built a firm foundation for cyber security. At the same time, it is clear from the report Cyber Security Assessment Netherlands 2016 that cyber threats are on the increase. Cyber crime, espionage and sabotage constitute a major risk for our economy and our society. If we are to remain a safe place to do business, we must respond effectively to these challenges. If it is to keep pace with the digital era, the Netherlands must take the next step, and it can only do so if government and business work together.

Patricia Zorko
Deputy National Coordinator for Security and Counterterrorism and Director Cyber Security at the Ministry of Security and Justice

THE NETHERLANDS: A SAFE PLACE TO DO BUSINESS

WE MUST TAKE THE NEXT STEP TOGETHER

The government has also made additional investments in tackling cyber crime and in the National Detection Network, whereby government and business inform each other of current threats. And the House of Representatives has recently adopted the cyber security bill, which requires the government and vital sectors to report serious security incidents, so the NCSC is aware of risks to society and can offer advice and assistance. But this is no reason to be complacent. Other countries are also defining a cyber strategy and investing heavily in this field. The head start that we had in this field appears to be holding us back. We must not let this continue. If the Netherlands is genuinely to be a safe place to do cyber business, both government and business must invest heavily over the next few years.

Helping hand

Fortunately, more and more organisations are putting cyber security on their agenda. Here too collaboration is crucial, because the cyber security of larger businesses often depends on that of smaller businesses. Equally, the small business sector is one of the sectors that needs more support. Luckily we have large organisations like the Port of Rotterdam and Schiphol Airport that can help smaller businesses in the chain with their cyber security. These are great initiatives.

Where necessary, the government can also lend a helping hand, in partnership with business. The government must also take the lead on combating and preventing serious cyber crime and industrial espionage, for example. These issues go beyond borders and must be discussed at EU level. And when it comes to regulations, our job is to harmonise them as far as we can.

Serious investment

Herna Verhagen s report makes it clear what needs to happen to make the Netherlands more secure. I agree with her that there must be a greater focus on cyber security, in the House of Representatives, in the boardroom and in the home. We must all focus far more on cyber security and think about how we can keep ourselves cyber secure, especially now that more and more devices are connected to the Internet. We can no longer afford to be naive. I also believe that the benchmark of setting aside 10% of your ICT budget for cyber security is a good rule of thumb for all of us, and makes a start on serious investment in your own cyber security and the cyber security of the Netherlands as a whole. We must also invest more in education: in teaching basic cyber security skills and in producing cyber security specialists to ensure that we continue to meet the growing demand in this field.

Time to act!

There s a lot of work to be done and everyone in the Netherlands must play their part. What we need is an overarching vision, ambition and strategy that everyone can engage with and act on. This action is crucial. We must identify where innovation is required and find the innovations that can take our country forward. That way we can exploit the opportunities that digitalisation offers and tackle the threats that come with it too. Government and business must work in partnership to ensure that the Netherlands continues to be cyber secure in the future too!

Jos de Groot
Director, Telecom Market, Directorate-General for Energy, Telecommunications and Competition, Ministry of Economic Affairs

THE NETHERLANDS MUST LEAD THE WAY ON CYBER SECURITY!

Recently, the Ministry of Economic Affairs has been focusing increasingly on cyber espionage that is targeted at innovative Dutch businesses, which is clearly on the increase. The same applies to the threat of cyber attacks on vital infrastructures. The failure of key infrastructures such as energy and telecommunications is unthinkable. It would cause major disruption to our society and our economy.

The good thing is that now, in my capacity as director of telecommunications policy, I can use my experience of policy in the energy sector to minimise the risk of these kinds of scenarios in these sectors. But this can't be done if we don't work closely with the business community, so I'm delighted with the recent report by Herna Verhagen, CEO of PostNL. She emphasises that cyber security is a prerequisite for economic growth and social development. And she makes a number of recommendations. Which recommendations interest me in particular? Lots of them interest me but I will focus on just a couple here.
Given that the Netherlands is keen not only to retain its competitiveness and keep its business climate in shape but also to exploit the economic potential of cyber security, there's plenty of work to be done.

Knowledge development

The first recommendation that interests me in particular is promoting the development of knowledge in the field of cyber security. Delivering innovative products and services is a race to the top. If we are to win this race, it is crucial that we not only develop knowledge but that we rapidly apply it to business. Only then can businesses deliver more state-of-the-art products and services that prevent damage and offer economic opportunities. And these opportunities do exist. In recent years, the turnover and added value of cyber security within the ICT sector has grown by 14.5% a year.

Secure hardware and software

Insecure hardware and software is often referred to as the Achilles heel of cyber security. There's no doubt that with the advent of the Internet of Things, the impact of vulnerabilities is becoming increasingly obvious. That takes me to my second point. In conjunction with the business community, the Ministry of Economic Affairs is already focusing on improving the security of hardware and software. By defining a framework for the development of secure software, for example, but also by promoting innovative, secure products. But we need to do more. In collaboration with the Ministry of Security and Justice and the business community, we want to create a roadmap for secure hardware and software. This roadmap will identify the tools we should use to improve the security of the Internet of Things, for example, so we are properly informed before we take the next steps, at both national and international level.

Cyberwise

Making the Netherlands cyberwise is the final point that I want to touch on. For me, cyberwise means being aware and being able to act appropriately. Information campaigns targeted at SMEs and the public as a whole are a key factor in this. Together with its partners, the Ministry of Economic Affairs is supporting a number of initiatives in this field, such as the website veiliginternetten.nl. One of the Ministry of Economic Affairs' priorities is finding ways of making small businesses more cyber secure. It's good to see that large businesses are already helping smaller businesses in their production chain. We ourselves are looking, amongst others, at further expansion of the Information Sharing and Analysis Centres, so that, in addition to vital sectors, non-vital knowledge-intensive sectors can also be involved.

A great many good initiatives are already under way, but if we are to tackle the threats and exploit the opportunities we must do more. We have shown as a nation that we can win the fight with water. Let us now do the same in the fight with cyber security!

"Delivering innovative products and services is a race to the top. If we are to win this race, it is crucial that we not only develop knowledge but that we rapidly apply it to business."

Ronald Prins
Chief Technology Officer &
Founder Fox-IT

The elections are just around the corner. Not only in the Netherlands but also in France and Germany. According to Ronald Prins, these countries must take it as read that there will be cyber breaches of the press and in political environments. "The signs are already there." He is calling for the appointment assignment of a high-level Cyber Commissioner who, just as the Delta Commissioner builds flood defenses, builds defenses in the interests of our national security and ensures that we exploit the economic opportunities that are available to us. "If we're not careful, we will be excluded."

INVEST IN A DIGITAL BUSINESS CLIMATE

"The Russians regard influencing other countries through cyber attacks as a game, and their success motivates them to devote even more energy to it. This won't necessarily happen in the Netherlands or be on the same scale as it was in the US but, rest assured, it will happen." Prins is convinced that if Fox-IT does research, it will find something in political parties, whether it be in the present or in the past. And it's not just the Russians who want to exert their influence. "The Turks are also active in this field. They want to know what direction we're heading in. We've already seen incidents of this nature." Talks are currently under way between the intelligence services and the business community to defend the Netherlands against cyber influencing. But Prins would prefer it if there were no electronic elections at all. "I've been trying to explain the risks associated with this for a few years now and I regularly get the response 'Be realistic, who would want to hack the Netherlands?' In my view, that argument has had its day and everyone needs to realise that as a digital society we are extremely vulnerable."

Cyber Commissioner

According to Prins, the fact that, as a digital society and a digital economy, the Netherlands is highly vulnerable is reason enough for the new government to appoint a Cyber Commissioner. "We need someone in a high-level position with a mandate, a budget and a department that makes serious plans. At the moment, what we have in the Netherlands is a cyber security strategy that combines action plans for things that are already in progress. That must change!

So it's important that the Cyber Commissioner has powers across all departments. Cyber security is such an urgent issue that we can't embark on a long-winded consultation process. As Delta Commissioner, Wim Kuijken sometimes makes decisions that not everyone agrees with. He has the powers to do so. And the Cyber Commissioner must have the same." And, says Prins, the powers of this new Cyber Commissioner must also extend to the business community. "Businesses will just have to get used to cyber issues being regulated from above. Our vital infrastructure, for example, is already a regulated sector to which government regulations apply. So, why shouldn't this be the case with cyber security?
Maybe companies feel as though something is being imposed on them, but what I would really like to see is the Cyber Commissioner taking

responsibility for what goes on in the business community and showing leadership that is based on an overarching vision and ambition. That way it wouldn't just be one party forcing something on another, it would be both parties working together to achieve a specific objective. In a nutshell, the Cyber Commissioner would have overall responsibility for cyber security in the Netherlands."

Digital business climate

A Cyber Commissioner would be in an ideal position to make the link between cyber security on the one hand and economic opportunities on the other. Prins: "The Netherlands is a trading nation, and we are extremely dependent on our digitalised economy. The whole of our horticultural sector is dependent on the Internet: if the Internet goes down, we won't be able to even harvest a cucumber. This has its advantages. Potentially we can play a leading role in the field of cyber security at European level, and maybe even at global level. Companies will increasingly be on the lookout for a secure country where they can base their data centres and their IT. They will look to countries where they are least likely to encounter problems and where the government offers assistance, in the form of a safety net in the event of a disaster and as an initial filter for the prevention of incidents." According to the founder of Fox-IT, the new Cyber Crime Act III and the Intelligence and Security Services Act will be instrumental in creating an attractive digital business climate of this type for businesses. "Internet Service Providers may find it annoying that their signals can be tapped or hacked as a result of this legislation, but our national banks are quite happy about it. Generally speaking, businesses are quite happy for the government to protect them from foreign hackers and foreign powers. They are not afraid of our government intervening in their networks. If we don't work together and jointly invest in the creation of a cyber secure business climate, I fear that we will be excluded. If Germany, for example, says to our businesses: 'Why not come here, we'll protect you from the Chinese,' then they'll go over the border. In my view, from an economic security perspective, it's not such a bad idea to let the Ministry of Economic Affairs take the lead on this. After all, it is in the ideal position to see the economic opportunities and take advantage of them."

Decision-making

One slight problem is that the Netherlands is likely to face a shortage of cyber security experts.

Prins acknowledges that this is an issue but believes it's because too little attention is paid to cyber security in the Netherlands. "If we tell people that our ambition is to make our country cyber secure, they will rise to the challenge. Young people will study the subject if they know that a good and challenging profession awaits them. The main problem at the moment is that decision-makers have to make decisions about something that they don't properly understand. A judge will have no problem telling a hacker that as a punishment he can't access the Internet for two years. But he doesn't understand that in our digital age this is a very severe punishment and that it may adversely affect the young man's digital literacy for the rest of his life. How should such a judge weigh up the proportionality and subsidiarity of a planned interception? Education will help but I believe that the problem won't be solved until future generations. Generations that grow up in a digital world and who have the digital literacy that goes with it. It's also important that they are given proper training in this field at school, and that they learn digital standards and values."

Warning

Finally, Prins warns against complacency in the Netherlands. "Are we really doing things quite as well as we think? Take the Internet of Things (IoT), for example. If we connect everything to the Internet in an insecure way our society will become increasingly vulnerable. It's awkwardly quiet here at the moment but this is a very worrying trend. More and more countries will realise just how powerful and cheap cyber warfare is. Both foreign regimes and terrorists. So we must prepare ourselves effectively."

A high-level Cyber Commissioner who, just as the Delta Commissioner builds flood defences, builds defences in the interests of our national security and ensures that we exploit the economic opportunities that are available to us.

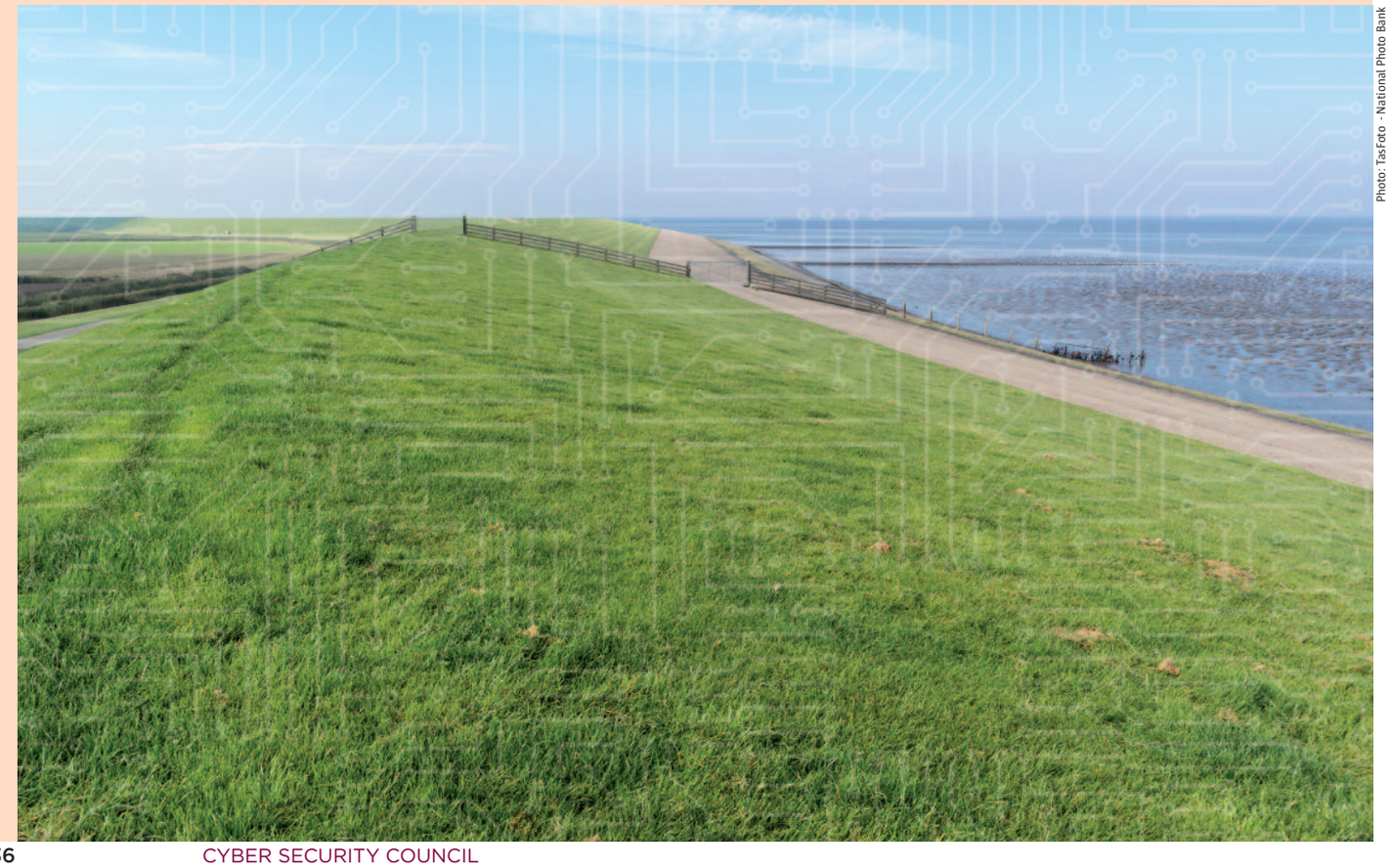
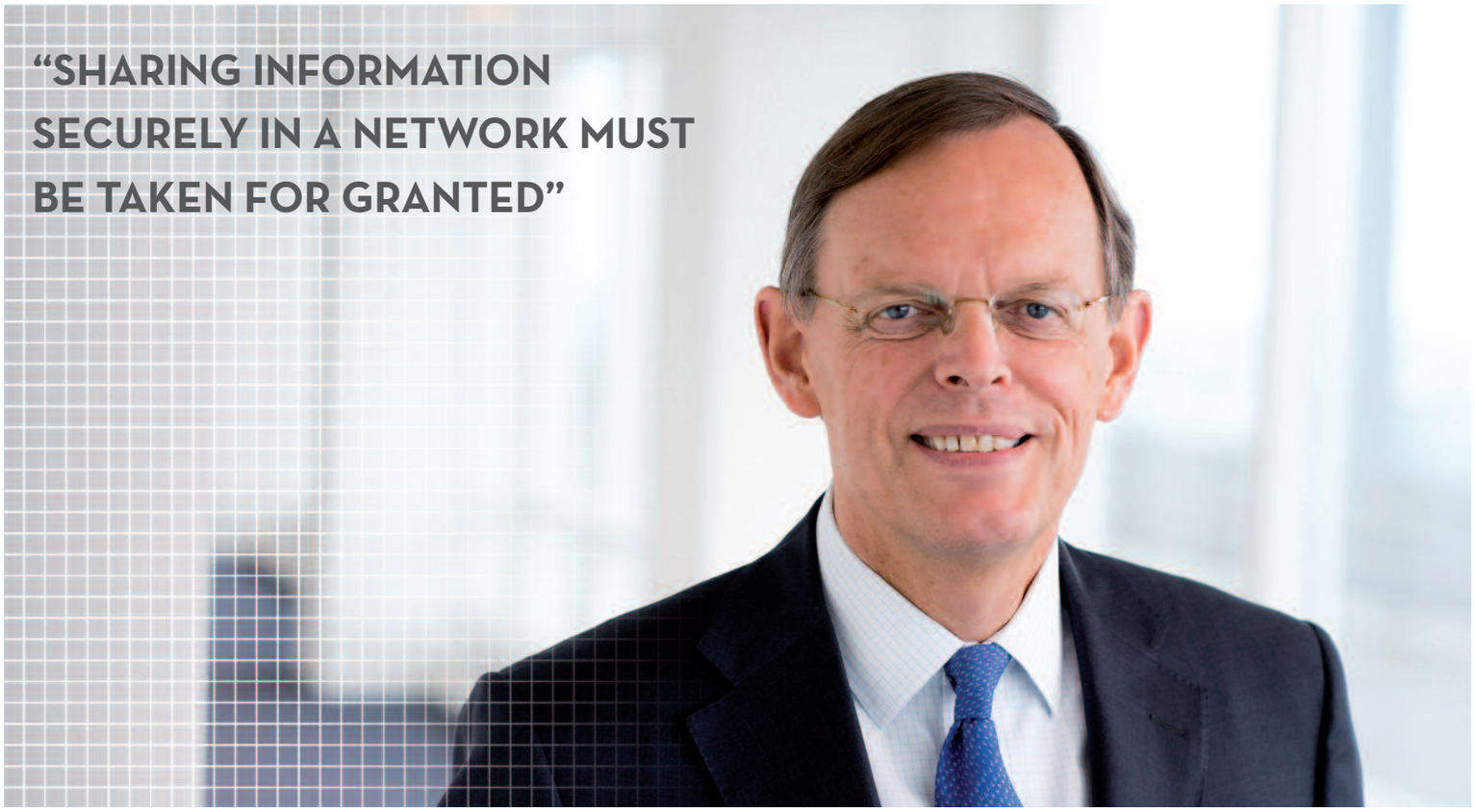


Photo: TasFoto - National Photo Bank

Hans de Jong
Chairman of the Board and CEO of Philips

TAKING THE NETHERLANDS FORWARD THROUGH DIGITAL TECHNOLOGY



We must talk openly with each other about the importance of cyber security, collaborate more closely with each other and structure our work in this field. That way we can take a digital quantum leap together.

One thing you can never say about cyber security is: we've got it sorted. What's good enough today will be superseded tomorrow. That's why the government, business and consumers must work together to ensure that our cyber defenses are the best they can possibly be. The entire world is facing this challenge, and that offers huge opportunities for a leading digital nation like the Netherlands.

Collaborating in a network

Here at Philips, we believe that it's important to be able to guarantee the cyber security of our professional and consumer products and solutions. Particularly since they often involve medical equipment and personal healthcare solutions. In order to achieve this, it's also important for us to be able to guarantee cyber security within our own organization. We work with others in a chain that extends from our suppliers to our customers. But chains are only ever as strong as the weakest link. That's why, for us, the cyber security of the entire chain is crucial. As a result, we place stringent

“Secure Digital technology offers huge opportunities for the Netherlands”

requirements on our partners to ensure that the security of their systems is and remains effective. And we help them by sharing information with them and by referring them to the appropriate tools and partners. Not all businesses, particularly small businesses, find it easy to keep pace with developments in this field. That’s why we share our knowledge on a voluntary basis with our partner companies. In the high-tech Brainport region, for example, we have taken the initiative, in conjunction with chip manufacturer ASML, to collaborate with what is now more than 25 businesses: we keep each other up to date with the latest opportunities in the field of cyber security and notify each other of attacks. It must also be taken for granted that governments will take part in these kinds of networks. Philips is also active within National, European and International working groups on security.

Security-by-design

More and more products are connected to the Internet. In the case of health-related products, the difference between use of a product for healthy living and use of a product to stay healthy after an illness (e.g. a heart problem) is becoming increasingly blurred. One example of this is the use of health watches. Access to and use of data is sensitive, so it’s essential that cyber security is automatically incorporated into everything that is developed (security-by-design). And it’s not only effective design and testing that is important but of course also being able to respond quickly and effectively if, in spite of this, something does go wrong. Nowadays, for companies like ours, quality is about more than just the correct functioning of products and services. It’s also about safe use. Confidence in the secure sharing of data, amongst both professional and individual users, is essential. Enabling this is a crucial part of your work.

eHealth

Moreover, consumers themselves also play a key role when it comes to their cyber security. When we supply equipment to hospitals or care institutions for example, we make sure that it is secured in the best possible way against hacks and attacks. But if outsiders, for example, can easily gain physical access to the equipment, or if staff stick their passwords on their screens or are not properly aware of the risks, however well protected a system is, it will still be vulnerable to those with malicious intent. I realise that most institutions (hospitals, educational institutions etc.) are taking measures in this field. But with the advent of eHealth, the Internet of Things and all manner of new applications for individual consumers, the battle against cyber crime must be waged on ever more levels. So, we must really focus on raising awareness among users. In my view, the government has a key role to play in this, as do businesses in terms of their internal communications.

Framework of standards

If we are to be able to take full advantage of digitalization as a nation, the first thing we must do is make children digitally literate from an early age and teach them about the opportunities and challenges of the digital world. And because digital developments evolve so quickly, the same actually applies to the generations who have already left school. Secondly, as well as focusing on raising awareness, the government must also strive for an integrated approach to cyber security. Clearly, each department will have its own responsibilities but there must be more collaboration between them. In my view, the key factor here is not legislation but a framework of standards linked to certification, for example. This can be done, for example, by focusing far more on public-private partnerships. Large companies like Philips have been sharing information and experiences with authorities for decades. But this must be intensified at operational level. The recent Ministry of Defense exercise involving a fictitious cyber attack in which a number of companies with expertise in this field took part is a good example of this. You don’t have to divulge details of all your critical processes and business information to each other to do this, but you can learn a huge amount from each other.

Digital quantum leap

Here at Philips we are all too aware that nobody can fight cyber crime on their own. The government, businesses, institutions, knowledge institutes and citizens must all play their part. Our success will be determined by the extent to which we learn to collaborate. I am convinced that if we combine and structure all the individual knowledge and experience that we have acquired in the Netherlands in the field of cyber security, we can take a digital quantum leap. We must also broadcast this ambition. Secure digital technology has huge potential to help solve social challenges in the field of healthcare, mobility etc. As a nation, we must resolve to lead the way in this field. We are quite capable of doing so. This offers huge economic opportunities. Opportunities that will enable us to take our nation forward for future generations.

“The government must invest in an integrated approach”

Photo: Kees Looijesteijn - National Photo Bank

If outsiders, for example, can easily gain physical access to the equipment, or if staff stick their passwords on their screens or are not properly aware of the risks, however well protected a system is, it will still be vulnerable to those with malicious intent.

When people think about security at Schiphol they usually think about the security staff in the departure hall and the police officers who keep all these millions of passengers safe as they travel through Schiphol day in, day out. But cyber security is just as important. If we can no longer rely on the Internet because it is no longer secure or because digital services fail, we will be extremely vulnerable. We must prevent this by investing heavily in cyber security measures.

Jos Nijhuis
President and CEO of the Schiphol Group

IS OUR DIGITAL BIKE SECURELY LOCKED?

Anyone who uses the Internet must understand that online security is no different to offline security. Whenever my three children went off on their bikes, I made it clear to them that they must lock them up. And depending on where they were going, I also told them to take a chain with them so they could chain their bikes to a railing of some sort.

Cyber aware

I wonder however whether we as parents and schools focus sufficiently on the security of our 'digital bikes'. Do teachers even know how to 'lock' them? Do they talk to their pupils enough about this issue? After all, cyber awareness must be instilled in children from an early age. I'm also concerned that our universities are not producing enough cyber security experts. We're not likely to be able to keep one step ahead of cyber criminals in all areas but shouldn't we at least try to keep pace with them? I believe that we can do this if we invest in education in this field and if we make it 'sexier' for young people to become cyber security professionals. This is an ideal task for the government and it would seem to me to be an excellent starting point for the Cyber Commissioner that Herna Verhagen calls for in her report.

Rule of thumb for ICT budget

I'm not suggesting however that the private sector should let the government shoulder all of the responsibility for cyber security. We have a responsibility too. I therefore fully endorse the recommendation in the report that, as a rule of thumb, 10% of your ICT budget should be reserved for cyber security. If you set it lower than this, there's a strong possibility that it won't be enough. I'm not saying that that precise figure should be set in stone but the very fact of using it as a benchmark forces you to take the matter seriously. That way, we can prevent cyber security being an afterthought and we can ensure that cyber security becomes an integral part of everything that our business does in the field of digitalisation. And if larger companies, which are often well aware of the importance of cyber security, give smaller companies a hand that can only be a good thing.

Third mainport

It is not enough just to look to education and to the future, we must also consider the present. Like the Port of Rotterdam, Schiphol is regarded as a mainport, i.e. vital infrastructure for the Netherlands. Wouldn't it be great if the digital economy, which is growing faster than any other sector, were to be designated as the third mainport with a Cyber Commissioner as champion? And what a bold move it would be if the new government were to take on this responsibility. And, in my view, the government should also create a climate in which there is an incentive for businesses and organisations to report issues in the field of cyber security. Because, if we are to catch up in the field of cyber security, we all need each other. It is crucial that the new government realises this and acts accordingly. While our politicians continue to make mistakes with their own use of emails (in other words they fail to lock their 'digital bikes' up properly) we can conclude that there is still work to be done in the field of cyber security in all layers of our society.

"Cyber Commissioner as champion of digital economy is a great idea"

“And what a bold move it would be if the new government were to take on this responsibility”

The Netherlands is a trading nation and we adopt new technologies quickly. Schiphol is a prime example of this. It gives us an edge. But as a result, we also encounter the challenges of cyber insecurity first and perhaps to the greatest extent. So we must strengthen collaboration between the private and public sectors and intensify research around cyber attacks in order to ensure a faster response and better prevention. And we must make the Netherlands cyber secure and cyber aware.

Security within the chain

It’s not only the government that has a responsibility to make the Netherlands cyber aware, we all have a responsibility in this regard. Schiphol has set itself the goal of being the ’best digital airport’ in the world. That means investing heavily in our ICT and consequently also in our cyber security. This is just as essential a part of our processes as physically checking whether passengers have a bomb on them. We are working very closely with a wide range of partners in our chain (customs, handling companies, airlines, the Dutch rail operator NS etc.) with whom we need to be to able to share information and data securely. We can only do this in a digitally secure environment. That’s why we don’t just ask our subcontractors: “is everything in order?” We look with them at how things could be better, what the ideal scenario is, and how we can achieve it together.

Ecosystem

To this end, we have set up the Cyber Synergy Schiphol Ecosystem (Cyssec), a platform that provides organisations at Schiphol with tools to help them promote cyber security. The purpose of this platform is to improve our overall resilience in terms of cyber security by sharing knowledge and information and exchanging best practices with four hundred partners. This year, we also plan to hold a joint cyber exercise. After all, the chains within which we operate are only as strong as the weakest link.

As Herna Verhagen said in her recent report on cyber security, the digitalisation of the Netherlands brings with it huge economic and social opportunities. In this context, confidence in the digital world is crucial. Consequently, she rightly calls on the government and the private sector to take action as a matter of urgency to improve cyber security in the Netherlands.

Johan Arts
Vice President IBM Security Europe

ARE WE LOOKING FOR CYBER SECURITY EXPERTS OR ROCKET SCIENTISTS?

TECHNOLOGY ENABLES CYBER EXPERTS TO BE DEPLOYED QUICKLY AND EFFECTIVELY

The serious shortage of cyber security experts is potentially a huge problem. The leading security organisation (ISC)² predicts that by 2020 there will be a global shortage of 1.5 million specialists, with security analysts being the most in demand. 46% of all the organisations questioned said that they were already experiencing a shortage in this field[1]. There are no specific figures for the Netherlands, but on the basis of our GNP, there is an estimated shortage of around 20,000 experts.

Shortage of courses

Why is this? The shortage is caused by a number of factors. Not only is there a shortage of courses in this field but we are now paying for a historical shortage of trained specialists. Moreover, in order to be of benefit to the security sector, you have to be highly educated, undertake refresher training on an ongoing basis and have a considerable amount of experience. It's almost as if you need to be a rocket scientist. So, as well as a shortage, there appears to be an issue with accessibility.

Technological innovation

In her report, Herna Verhagen calls for more investment in cyber security education, and I fully agree with her on this. But more and better education will not be enough and will not bear fruit for five to ten years. So, what do we do in the meantime? Can we use technology to make access to the field easier? Is this a realistic expectation? Personally I believe it is.
There are plenty of examples of technological innovation improving access in other professions and industries.
Take the following simple example: In the olden days, if you wanted to have a photo taken you had to go to a photographer, a specialist with experience, training and equipment.
Nowadays everyone takes their own photos on their smartphone. But photographers haven't just disappeared, they are concentrating on more specialised projects, such as fashion reports or portraits. The expert in the field moves into a more specialist area because some of the work can be done by people with less training and experience. If you translate this

> “The use of artificial intelligence would get more people into work in the cyber security sector more quickly”

simple example into today’s work environment, the implication is that technology will enable more experts to be deployed more quickly and more effectively.

Human experts

Cyber security can also use technology to lower the barriers to entry of education and experience. Take, for example, the structure of the Security Operating Centre (SOC), a key component of any security organisation: A level 3 SOC analyst normally has an in-depth technical background and more than ten years of cyber security experience. A level 1 SOC analyst can’t just take over the work of a level 3 SOC expert. But could this happen in the future?
To answer this question, we have to understand how and why it is so difficult for people to enter this specialist field. Despite the fact that it is a technology-orientated field, it appears to be highly dependent on human experts. The stringent entry requirements have arisen because information on cyber security is provided in a fragmented and unstructured way. Specialists accumulate their knowledge by engaging with the security community for many years, by reading blogs, following experts and attending conferences, for example. But even for specialists this is becoming an increasingly thankless task, because every year more than 700,000 security blogs and 10,000 research documents are published.

Cognitive technology

Cognitive technology can help access huge amounts of unstructured data, such as blogs, at superfast speed, and distil knowledge from it that is made available to cyber security specialists by means of a digital adviser, for example. As a result, junior specialists like the level 1 SOC analyst gain immediate access to up-to-date knowledge that they would otherwise only have been able to acquire through many years of experience.
Recent tests in European countries, including IBM’s Watson for Cybersecurity technology, indicate that applications of this type actually help detect incidents more quickly. I would like to stress that this is not a pipe dream, it is technology that already exists.
All of this helps specialists in all fields to detect cyber incidents more quickly and, more importantly, to solve them more quickly. And, according to the IBM Institute Of Business Value’s recent report *Cybersecurity In The Cognitive Era*, alongside the shortage of cyber specialists, this is one of the key priorities of Chief Information Security Officers (CISOs). This study, which is based on interviews with seven hundred CISOs from 35 countries and 18 industries, indicates that reducing average incident response time and resolution times is the key challenge over the next three years[2].

Artificial intelligence

Whenever the subject of artificial intelligence comes up, people always talk about unemployment: will the use of artificial intelligence lead to job losses? At the moment, the shortage of cyber security specialists is so significant that there is no question of this. Moreover, the use of artificial intelligence would get more people into work in this sector more quickly. We will still need human intelligence and, more particularly, human intervention to protect our IT infrastructure in the best possible way and to be able to respond to breaches.
In the long term, I foresee that the symbiotic relationship between humans and machines will only get stronger and we must be careful not to get too fixated on the word ‘artificial’: it’s more about the ‘augmentation’ of human intelligence.

Confidence in the digital world

Here in the private sector we must therefore use our innovative capabilities to provide cyber security specialists with new tools to help them achieve their objectives, thereby enhancing confidence in the digital world.

Notes:

1. The 2015 (ISC)² Global Information Security Workforce Study, 2015
2. Cybersecurity In The Cognitive Era, IBM Institute Of Business Value, 2016

The digitalisation of our society is progressing at lightening speed. At the request of the Dutch Cyber Security Council, the CEO of PostNL, Herna Verhagen, has written a report that indicates that – in almost every sector of society – digital technology is the primary and most important means for processing and sending information, and for controlling processes. "It is a recognizable phenomenon; we see it reflected in Nationale-Nederlanden's strategy. In summary: digital, personal and relevant. Before we develop a new service for customers, we ask the question if we can offer the new service digitally", says David Knibbe CEO of Netherlands Insurance ('Nationale-Nederlanden') and Chairman of the Dutch Association of Insurers.

David Knibbe
NN Group's CEO of Netherlands Insurance

TAKING A STAND FOR THE SAFETY OF SMALL AND MEDIUM-SIZED ENTERPRISES (SMES)

According to David Knibbe, a focus on digital security is extremely important for businesses. "Companies are becoming more information- and IT-driven. That means that top management should continue to address the protection of critical assets. In our case, the personal and financial data of our customers,' he says. 'Within NN, we have an over-arching security structure, which is implemented in every business unit. We have a Chief Information Security Officer, who is responsible for the overall security of NN Group. And there are local security teams, led by Business Information Security Officers, in every business unit."

The right sparring partner

"Centralised control and coordination are crucial for an effective approach," David continues. "That means that everyone – not just Boards of Directors and Supervisory Boards – must delve into security risks and must be aware of their responsibilities and liabilities. It applies to everyone within a company. After all, these are precisely the aspects that get plenty of media attention after a hack or a data leak. It also means that security officers should provide the top executives in their company with up-to-date information and relevant issues. For executives, these officers are useful advisors and sparring partners. Within Nationale-Nederlanden, we also use ongoing security scans and employ security guidelines that our businesses must meet in order to properly protect data. Think of encryption and supplementary digital surveillance. While in big companies, cyber security is often already well-established, most smaller companies still have some work to do."

"Centralised control and coordination are crucial for an effective approach."

SMEs as an attractive target

The Cyber Security Council's report suggests that in the Netherlands SMEs are less secure, and therefore an attractive target for cyber criminals. "Many entrepreneurs are not even aware that they've been attacked by hackers. Sometimes, hackers can be active within their systems for months, and may cause irreparable damage, before an entrepreneur finds out. It is therefore crucial that we better inform SMEs about cyber security. And by the way, it's not enough to simply lay the responsibility for cyber-safe SMEs at the government's feet. Even when extra funds are made available for that. Just look at the results of the most current cyber-security grants: despite the best of intentions, 2016 saw a record

> “Small businesses benefit from security solutions that are tailored to their situation”

number of data leaks and cyber-crime activities. ‘More money’ is therefore not always the solution. There’s much more that should be done. All the key players must work together: commercial and non-commercial, multinationals to start-ups. Everyone can contribute from his or her own area of strength: whether that's knowledge or network or another strength. It’s all about working together.”

SME support

“SMEs will benefit from security solutions that are tailored to their specific circumstances, and from targeted support in making the right choices from among the options available. Entrepreneurs are confronted with all kinds of changes in nearly every aspect of their business. They work hard, seven days a week, and sometimes they barely have time to check their own IT system. Often, they also don’t have the financial or human resources available to invest in security,” David says. “In that respect, an SME entrepreneur’s world is very different from that of the CEO of an international organisation. The general guideline of spending 10% of the IT budget on security is likely not feasible for all entrepreneurs. For SMEs, support should be all about accessibility, affordability, and a positive image regarding security awareness. It’s not about intimidation, but rather about simple communication, clear language, and brief explanations – with examples and without jargon.”

Dutch Cyber Collective

In late November, stakeholders took the initiative to establish the Dutch Cyber Collective. It is an independent platform that aims to connect everyone who has an impact in the cyber world. In addition to Nationale-Nederlanden, companies such as Deloitte, ESET Netherlands, Fox-IT, Report Crime Anonymously, Threadbare Stone Cyber Security, and Safe Internet have all joined the collective. The Dutch Cyber Collective swiftly tracks new cyber attack methods, through the partners and directly through the SMEs themselves. Every hack is a lesson, and is used to protect other SMEs.
“We know from experience that SMEs often don’t report cyber attacks. Perhaps because they’re afraid of reputation damage, or because they don’t want to publicise their weak levels of security,” David says. “But because of that, no one can learn from the attacks, and cyber criminals can continue to exploit similar weaknesses among other SMEs. Incidentally, if so-called sensitive data is captured, this should always be reported to the Authority for Personal Data (AP). And, depending on the type of information, this must also be reported to the people whose information has been leaked. Of course, we hope that SMEs contact the cyber guard if they are hacked. This guard is part of the Dutch Cyber Collective. But obviously, we prefer to engage before-the-fact, and help SMEs become digitally safe(r).”

Joining forces

“The Dutch Cyber Collective’s primary objective is to turn the current fragmented approach into a consolidated whole, and to make the Netherlands safer when it comes to cyber security. We’re therefore completely aligned with the Cyber Security Council report,” David continues. “I am calling on all interested organisations and individuals to collaborate with the independent Dutch Cyber Collective. That’s how we can join forces to take a stand against cyber criminals. It goes without saying that the Cyber Collective is also keen to work with, or contribute to, other political or governmental initiatives. Cooperation, coordination and information – these are the keywords for making the Netherlands digitally safer in the short term.”

The Netherlands is a water-rich nation. An inherently risky environment. In this risky environment we don't build fences around every river, canal or lake. That would not be practical, it would create a false sense of security and it would also be too expensive. So what we do is send our children for swimming lessons, so they learn how to manage the risks of living in this water-rich nation. And we must also use this approach as a model when we consider how to manage the inherent risks of our digital environment.

Dick Berlijn
Cyber security advisor, Deloitte Nederland

WE DON'T SEEM TO BE SUFFICIENTLY AWARE OF THE RISKS

LEARNING TO SWIM IN THE DIGITAL SEA

You could put a fence round every piece of data but it wouldn't be practical and it would create a false sense of security. The better option would be to teach every Dutchman to swim in the digital sea. Over the years, Western societies have become increasingly dependent on digital applications, networks and data. It's only in the last ten years, following news of the many hacks and cyber crimes, that we have started to realise that this is not without risk. We are now entering the era of the Internet of Things, big data and data analytics. And, once again, we are tempted to jump in with both feet and to blindly embrace all the applications that this brings. And they are not insignificant. But, once again, we don't seem to be sufficiently aware of the risks.

Government must act as regulator

In my view, the greatest challenge is raising awareness of the issue and associating it with consequences, doing the right thing. In concrete terms, this means clarifying who is responsible for what, concluding agreements around who does what and putting cyber security on the agenda and keeping it there. Various parties have a responsibility in this context: we ourselves, as individual users of the digital environment, businesses, the government and many others besides. The government is already doing a great deal but must act as more of a role model. It's no longer acceptable for local authorities to still be using Windows 7, for instance. In addition, the government must act as a regulator and take us to task over our responsibilities. I believe we should also take more of a carrot and stick approach: people who don't take it seriously should feel the consequences, and people who get on with the job should be rewarded.

Digital defences

The level of cyber security in the Netherlands varies hugely from one sector to another. The financial sector has got its cyber security pretty much in order. Failing to protect itself adequately is just too expensive. But in other sectors there is often far less awareness of cyber security. For example, I am sometimes asked to talk to hospitals about this issue. These hospitals don't always realise that they are sitting on a huge amount of data. This data can be used for all kinds of good things, such as predicting the progress of a disease, research and better outcomes from operations. But hospitals are also vulnerable. Anyone can go in and out and data isn't always adequately protected. If you don't understand how important data is, you won't invest as much in security.

Secure

I'm certainly not advocating making everything as inaccessible as possible. The sharing of information is too important for that. But you need to be as prepared as you can be for potential hacks. Think about how you organise your digital defenses and what you want to put online or otherwise. You don't want to run risks that you don't have to run, so you need to take action on this. But 100% security doesn't exist, and keeping all doors tightly shut is not an option.

Vigilant

Is your detection capability adequate? Can your organization tell if unusual things are happening on its network? If it can't, your organization won't be able to take action either. An effective detection capability is therefore crucial.

Resilient

The next step is your response. Could your organization respond effectively if something unusual happened? Do you have a properly trained team that could respond effectively in the event of an incident? Could you keep the damage to a minimum? Or are all your eggs in one basket? Do you review your response after an incident? If so, you can also learn from the incident and modify your procedures if required.

“Cyber security is complex but tackling it is not difficult”

Resources

Small businesses won't always have sufficient resources to take all the measures that are required themselves. But the business doesn’t have to do everything itself, some aspects can be outsourced. All businesses, including small businesses, must review their internal organization: how do I use the Internet and what risks am I running? If you can't do this yourself, you should seek help from the experts. There are plenty of them around. Don’t ever think that you will not be effected.

Clear approach

Keeping pace with cyber criminals is a challenge. Here at Deloitte we do everything we can to build on our knowledge and experience in this field on an ongoing basis. Amongst other things, this means that we devote a lot of time to the recruitment of experts, mainly young people. To keep them up to speed we – amongst other things - send them to the Cyberlympics (annual international cyber security competition), where they’ve won first prize on five occasions. We are also subjecting our own organization to ‘self inflicted fishing campaigns’, in order to maintain a high level of awareness in this field.

Finally

Cyber security is complex but there are things we can and should do. What data do we have at our disposal, is all the data equally important, what data must never be compromised, how is this data protected, what about our identity and access management, should this data be stored in the cloud or otherwise etc? It all starts with awareness, knowing that your data is the new gold and that there are people who want to get their hands on it. Good password management, keeping firewalls up to date, installing software patches in good time etc. are all key issues that don’t cost a fortune to implement. A lot is already going on in the field of cyber security. The government is hard at work, many businesses and organizations give it the attention it deserves, and citizens are increasingly aware of the risks that are associated with all these new opportunities. But we must go further. Cyber security must be an integral part of our day-to-day lives.

Who guarantees security when clients unintentionally open up their data to third parties? New market opportunities require collaboration on cyber security issues.

Wiebe Draijer
Chairman of the Executive Board of Rabobank

WORKING SECURELY AND CONFIDENTLY ONLINE, ALSO OUTSIDE THE BANKING SECTOR

"digitalisation presents major opportunities for business and for society at large. To benefit from these opportunities in the long term, we must be able to rely on the digital world and operate securely within it."

This sentence from Herna Verhagen's report couldn't be more to the point. Our day-to-day lives are increasingly supported and shaped by digitalisation. Cyber and offline tools and activities are fully integrated. It's also important to remember this when talking about security. Too much emphasis on words like 'digital' and 'cyber' will make people think that it's nothing to do with them.

The security debate primarily centres on technical aspects and key issues such as the systems and software required, how to create a secure network and how to identify users. When I look at the world from a banking perspective however I see a different, and perhaps bigger, problem and that is the issue of security awareness, of being cyberwise in our digital world.

Fraudsters don't always need high-tech tools

Banks are keen to implement the highest possible level of technical security, for online client identification for example. But even then things can go wrong, simply because clever fraudsters are able to deceive clients – and they don't even need sophisticated high-tech tools for that. In the offline world, skills and habits that feel totally natural to us often protect us from bad things like theft and fraud. The problem is that these skills are often lacking when we go online. And this has major consequences.

New market opportunities

The new European Payment Services Directive (PSD2) will offer opportunities for new entrants and promote a society that is based on an Open Banking Model. While this is good news for consumers, I do have my concerns, and that's not because these new regulations put pressure on the business models of banks. My real concern is that our clients will be extremely vulnerable if they unintentionally open up their data to third parties, or even get involved with peer-to-peer lending. Who guarantees security in these kinds of transactions? Who ensures effective protection for consumers against hackers? As the report says, the clients themselves don't have the necessary skills to protect themselves. And, other than issuing general warnings, as a bank we can't do anything to help because we are not party to the transaction.

Joining forces to improve security

In my view, there's a huge amount of ground to cover. The public and private sectors should join forces – to make our citizens sufficiently resilient, but also to ensure an effective regulatory environment without any deadlocks. For example, take privacy legislation or the statutory retention times for data. Only a coherent strategy for tackling these issues will allow us to build a secure future.

Fraudsters don't even need sophisticated high-tech means

I hope and expect that the new government appreciates the importance of a secure digital society, and that it will prioritise the cyber security agenda. The government should continue to invest in new, user-friendly security technologies while ensuring that we have an adequate supply of qualified security professionals in this country. And, finally, the government should organise public information campaigns around cyber security in conjunction with the business community. All of this is crucial if we are to operate confidently and securely in our digital world.

We have to make things harder for criminals in the Netherlands, including cyber criminals. Cyber crime costs Dutch society an estimated ten billion euros a year. The digitalisation of security has fundamentally changed the nature of policing.

Erik Akerboom
Commissioner of the Netherlands Police

VIGILANT AND EFFECTIVE, IN THE DIGITAL WORLD AS WELL

CYBER SECURITY IS TOP PRIORITY

The progress that we, as a police force, have made in the offline world in recent years must not be undermined by crimes that go unnoticed in the online world. As police force, we need to invest heavily in people and resources to keep pace with future developments. People must be encouraged to report cyber crimes, we need to constantly update our knowledge on cyber crime, and there investment in resources needs to be increased, so the police can do their work effectively.

Investment pays off

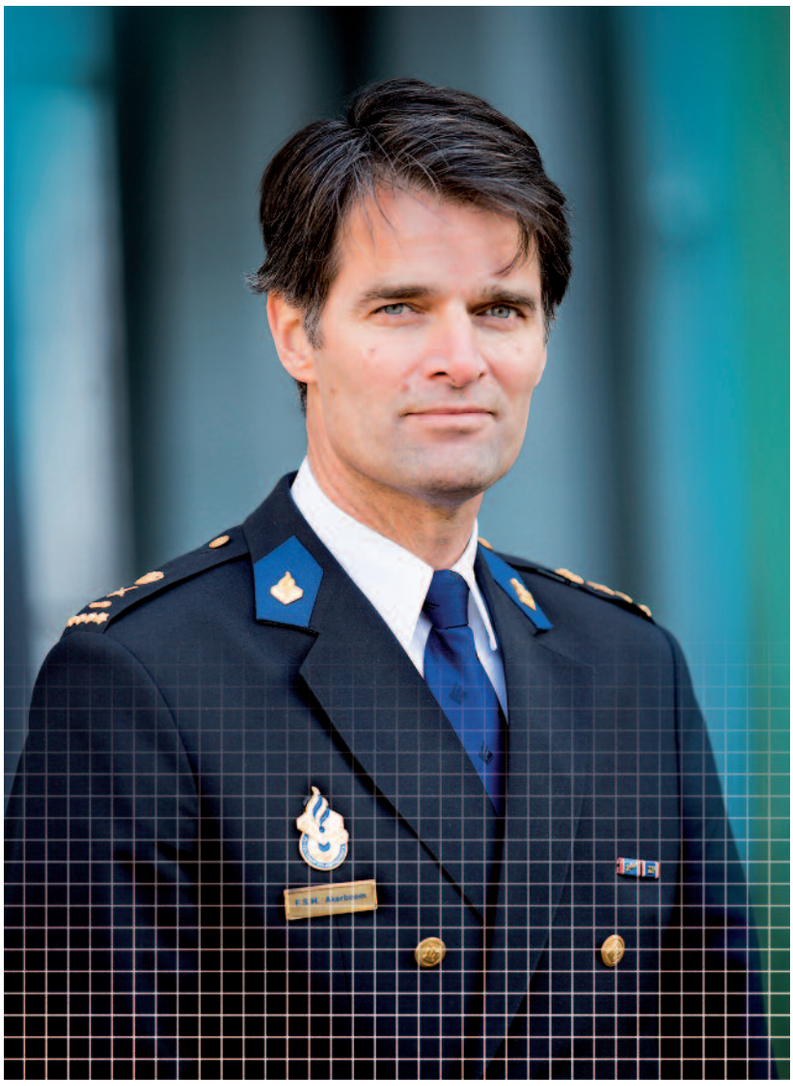
Our High Tech Crime Team (THTC), which has been fully operational since 2015, is evidence that significant investment pays off. The team is highly regarded internationally and, in recent years, has gained a great deal of experience through effective interventions and public-private partnerships. This year, the THTC successfully identified a Nijmegen-based company selling telephones to criminals. The phones enabled them to send fully encrypted messages. The company's 36-year-old owner was arrested and Dutch and Canadian servers were seized. But fighting cyber crime is no longer exclusively the work of a team of specialised colleagues. All 65,000 police officers must see it as part of their jobs. No matter whether they're on the beat, training our officers, working with European tenders or with ICT, tackling cyber crime is part and parcel of policing.

Tackling cyber crime effectively

For me, cyber security is top priority. I intend to create a well-equipped organisation that is vigilant and effective in the digital world as well. The first step on the road to tackling cyber crime effectively is to set up cyber teams within the units. This has already been done in some of the units, and the remaining units will follow suit. These teams investigate cyber crimes, raise cyber crime awareness amongst their colleagues in the units, and offer support to people reporting cyber crimes. This helps us improve the services we offer to citizens and businesses. The teams are essentially preparing the organisation for further digitalisation of policing in the future. In addition, between 2015 and 2018 we will recruit one hundred digital experts a year to help us tackle cyber crime.

Continuous upgrading

These are positive but basic measures. Given the urgency of the situation, we must also invest in a more user-friendly reporting process, well-trained personnel, a better intelligence position, and innovative solutions. To achieve this, there must be greater flexibility in the ratio between expenditure on personnel and resources, which is currently set at a fixed ratio in the budget. I would like this fixed ratio to be dropped. Moreover, if we are to keep pace with the current rapid developments, additional investments are required. The recommendations of the Netherlands Court of Audit on ICT in policing call for greater scope for the continuous



“Cyber crime is becoming a new service sector”

upgrading that is required. According to Ms Verhagen, a multi-annual action programme with an investment agenda in line with these recommendations should be put in place by the new government.

A modern legal framework is required

In addition to adequate resources, a modern legal framework is an essential prerequisite for the fight against cyber crime. Not only would this give us contemporary tools; it would also create parameters within which we can operate with democratic legitimacy. Current legislation and regulations are out-of-date. A first step in this direction is the Cyber Crime Act III, which was recently adopted by the House of Representatives and is now before the Senate. This law is vital for effective cyber crime investigation.

Government contribution is limited

According to the Dutch Cyber Security Assessment, cyber crime has significantly increased. There has been a dramatic increase in ransomware and advanced persistent threats in particular. Professional criminal groups are carrying out ever more advanced attacks. And the US recently saw the first large-scale DDoS attack using Internet of Things devices. Our High Tech Crime Team has its work cut out for them with these new innovative types of cyber crime, which are often directed at vital infrastructures. In this context it is important to realise that the government’s contribution to a guaranteed secure digital infrastructure is limited. We still have a huge step to take internally, but if we want to tackle cyber crime in the long term, we must work together with all relevant public and private partners. We must share our information with each other and must deploy all tools available in the interests of the Netherlands.

Opportunities for investigation

What I find worrying is that specialist knowledge is no longer required to commit cyber crime. Nowadays, you can buy complete packages on online marketplaces and use them to carry out a hack or a DDoS attack. And they even offer customer services.
Cyber crime is becoming a new criminal services sector. And crime increasingly comprises both the offline and the online worlds simultaneously. Drugs, weapons and false identity documents, for instance, are traded on the Darkweb. Payments are made with bitcoins, but the goods are delivered by couriers in the offline world. And the bitcoins are converted into euros. There are opportunities for investigation here. We are already working with couriers to intercept criminal packages. And our successful collaboration with banks will help us tackle this form of money laundering.

Public-private partnerships

Everyone is responsible for their own cyber security. We can only tackle cyber crime effectively if we work together with citizens and businesses to develop smart interventions. A good example of a successful public-private partnership is the Electronic Crimes Taskforce

Photo: Grekenrooi - National Photo Bank

Today's threats are tomorrow's regular crime. We must keep pace with the changes on an ongoing basis. If we don't invest in cyber security and fight cyber crime on a structural basis, we will not be able to keep up with these constantly changing threats.

(ECTF), which is a cooperative effort of the police, the public prosecution service, major banks and the Payment Association. In 2016, the ECTF organised an international money -mule campaign, which resulted in 178 arrests. And recently we entered into a successful partnership with security companies Kaspersky Labs and Intel Security in the field of Ransomware attacks. Information on preventing and remedying attacks of this type can be found on the website Nomoreransom.org. An increasing number of businesses get involved in this initiative. In addition, our National Internet Crime Reporting Point (LIMO) is cooperating intensively with banks and Marktplaats auction site to tackle fraud on online marketplaces. It also keeps records of sellers who have been reported as being fraudulent. 'Check de Verkoper' (Check the Seller) can be found on the Politie.nl website.

Systematic investment

Things change very rapidly in the field of cyber crime. Today's threats are tomorrow's common crimes. We must continuously keep pace with developments. If we don't pay attention to cyber security and cyber crime, we will not be able to keep up with its constantly changing threats. Neighbouring countries have made substantial investments in this field; the Netherlands must not lag behind.

"Neighbouring countries are investing heavily - the Netherlands must not be left behind"

As society becomes ever more digitalised, consumers become ever more vulnerable. Consequently, in order to protect consumers, we must draw up regulations. After all, we already have regulations that govern a product's physical safety and, in essence, our digital safety is the same.

Bart Combée
CEO of the Dutch Consumers' Association

CONSUMERS ARE ENTITLED TO EXPECT SECURE DIGITAL PRODUCTS TOO

Research conducted by the Dutch Consumers' Association indicates that consumers regard identity theft – password theft, phishing, passport fraud – as the biggest cyber security issue. This is also evident from the number of crimes reported by victims of identity theft. The problem stems in particular from the ever more professional nature of cyber crime: it is becoming increasingly difficult for the layman to recognise the various forms of cyber crime. The days of the blatantly obvious phishing email, full of spelling errors, are gone.

Lack of knowledge

Consumers are well aware of the problems and risks around cyber security. But it is often difficult for consumers to ensure that they are adequately protected because they don't have the specific knowledge they require to do this. That's because the situation is changing all the time and the issue is too complex. This does not however absolve consumers from their responsibility for their security. They must still install updates, use strong passwords and back up their data, for example. The Consumers' Association can provide tips and information on this.

Technology-neutral legislation

With the Internet of Things (IoT), things are changing so quickly that you can't expect consumers to be up to speed with everything. An incident such as the recent one involving smart toys secretly recording sound must not be possible. We are also seeing a waterbed effect in cyber crime: as soon as one sector is adequately protected, such as the banking sector, cyber criminals target other sectors. Because technology and crime are developing at such a fast pace, business and the government have an additional responsibility. The government must introduce technology-neutral regulations across the board. The next government must take up the challenge and put a strong legislative framework high on the political agenda. For example, it could be a requirement that the software, security and functionality of a product must be updated by the manufacturer during the lifetime of the product.

Mandatory regulations

In order to achieve the above, the government could require business to define its own regulations. An obligation of this type wouldn't be a bad thing: after all, you can't just set up a bank without a license and we also impose all kinds of requirements on physical products. It is unrealistic to expect companies to do this on their own initiative without pressure from the government. Firstly, it costs companies money to set up a system of this type and it doesn't increase their income, so they have less incentive to do it. Secondly, with a non- mandatory system, there is the issue of compliance. In other words, not all companies will

want to take part in a regulatory system of this nature. That way you only regulate the top of the market, not the bottom, which you need to do if you want to tackle the issues around cyber crime effectively. After all, consumers are entitled to expect properly functioning and secure digital products, just as they do with physical products.

Guaranteed security

From a consumer's perspective, I don't agree with the 10% benchmark that is recommended in the Verhagen report: consumers don't need to invest 10% of their budget in security. As a consumer in a modern economy you should be able to assume that any product that is available on the market is secure. This is essentially the same as for physical safety: you are not allowed to sell toxic products that require consumers themselves to ensure that the product is no longer toxic.

"The next government must take up the challenge"

Piet Mallekoote
CEO of the Dutch Payments Association

Secure payments systems are crucial for processing financial transactions efficiently. If security is jeopardised, it may result in a loss of confidence in the payments systems. This would lead to higher social costs and, in the worst case scenario, could trigger a financial crisis similar to the credit and debt crisis that we have experienced in recent years.[1]

CYBER SECURITY IS CRUCIAL FOR CONFIDENCE IN PAYMENTS SYSTEMS

GOVERNMENT MUST ENSURE THAT LEGISLATION AND REGULATIONS ARE WORKABLE

The digitalisation of the payments systems in the Netherlands has been under way for many years. The Netherlands is a European leader in this field and, as a result of this digitalisation, the social costs of payments in the Netherlands are amongst the lowest in Europe[2]. This cannot be achieved without complete confidence in the payments systems. And if this confidence is to be maintained, cyber security is crucial. According to the National Cyber Security Strategy's definition, cyber security is 'striving to prevent damage caused by disruption, failure or misuse of ICT and if, in spite of this, such damage occurs, rectifying the damage.' With ever more digitalisation and innovations in prospect, all stakeholders in payment systems must make cyber security their top priority.

> "Creating and memorizing different passwords is a thing of the past"

No longer adequate

All the parties involved in payment chains – providers, supporting service providers and end users – have a responsibility for security. This doesn't just happen. That's why the Dutch Payments Association and its members help raise awareness of online fraud among consumers and tell them what they themselves can do to prevent it. Take the high-profile national (TV) information campaign 'Hang up, Click it away!, Call your Bank', for example. Businesses can also do far more themselves to ensure that their customers can make payments more securely. For example, many e-commerce companies and utilities allow their customers to set up a direct debit by ticking a box in their online environment. However, from a cyber security perspective, this method, albeit cheap and effective, is no longer adequate, because the identity of the party that is setting up the direct debit is not established. That's why the Dutch Payments Association, together with its members, has set up a separate secure service for this (Digitaal Incassomachtigen – online direct debit mandates)[3]. So far, very few businesses are offering this service. Often businesses are still not sufficiently aware that security affects us all and that we must tackle it together, each from our own area of responsibility.

Intensively sharing information

Banks continuously invest in the security of the electronic payments systems by improving fraud and detection measures. Collaboration between the parties involved in the field of fraud prevention plays a key role in this context. Intensively sharing information with each other on threats, vulnerabilities and incidents enables financial institutions to take effective measures in advance. This collaboration takes place through the Dutch Payments Association and through public-private partnerships, e.g. with the National Cyber Security Centre (NCSC). This type of collaboration makes the Netherlands a leader in this field at European level. As a result of these partnerships and the greater public awareness of fraud prevention, losses caused by fraud in the online payments systems fell from 82 million euros in 2012 to less than 18 million in 2015. Over the same period, losses caused by phishing fell from more than 10 million to 3 million euros[4]. In 2016, there was a further decrease in fraud (10,2 million Euros).

Data security

Ever more data is stored and exchanged in digital form. This entails risks. So, if we are to digitalise further, it is crucial that we protect our data effectively. Banks do not exchange data with third parties. The online payment system iDEAL, for example, which is unique in Europe, has now been in existence for more than ten years and its security has never been compromised. This is partly because the personal login data that is required remains within the secure bank environment[5]. Based on these experiences, and partly on account of their social role, the banks decided to set up an online identification and login service. This service, which is known as iDIN, was launched at the end of 2016. iDIN allows individual account holders to identify themselves and log in online with connected organisations (merchants) using the trusted login method of their bank[6]. As a result, creating and memorizing different passwords for websites is a thing of the past. Not only is this more secure but often it's also far easier for users. iDIN gives merchants confidence in their online customers because banks have carefully identified their customers.

Principle-based assessment framework

The government can also use iDIN to speed up the planned secure digitalisation of its services. In this context, the government has decided to adopt a multiple method approach, which allows users to log in to government services using private as well as public methods. To this end, the Ministry of the Interior and Kingdom Relations has now published a uniform set of requirements and initiated a consultation on the proposed Generic Digital Infrastructure Act (Wet Generieke Digitale Infrastructuur). Unfortunately, rather than a principle-based assessment framework, the Ministry has opted for a set of extremely detailed rules including technical specifications (rule-based) which are not common in the market and of which, so far, no one has had any experience. An approach of this nature is surprising not only from an international perspective but also compared with other sectors such as online payments. Such a detailed approach also inhibits innovation due to its extremely limited scope. It will cause practical problems for private partners and will delay or obstruct the intended acceleration of the digitalisation of government services. The government would be wise to reconsider this approach and its likely consequences and to opt for a more principle-based approach that gives adequate scope for private partners to use their own methods and technology. The government must ensure that legislation and regulations are workable and involve market players in this process. This will be good for security and privacy.

Partnership

The Dutch Payments Association and the banks have been working in partnership with the government for many years now, with the NCSC, for example. This takes place, amongst others, within the FI-ISAC (Financial Institutes - Information and Sharing Analysis Centre) and essentially involves cyber threats and incidents being quickly and successfully shared between the participating partners and the sector remaining resilient as a result. Moreover, over the last few years there has been a special banks liaison that maintains contact between the financial sector and the NCSC on a daily basis. This has many benefits and results, amongst others, in the setting up of joint projects, such as the banks' participation in the National Detection Network and the National Response Network. If the financial sector is to remain secure, these activities are crucial. The advice to the government in this context is therefore to continue to give them sufficient priority over the next few years.

Notes:

1. Butter, Frank den and Mallekoote, Piet (2016) Vertrouwen in het betalingsverkeer: de rol van transactiekosten (Confidence in the payments system: the role of transaction costs). Economisch Statistische Berichten No. 4740, 11 August 2016.
2. DNB (2012) Kosten Nederlands betalingsverkeer behoren tot de laagste in de EU (Costs of Dutch payments system are amongst the lowest in the EU). DNB press release 20 December 2012.
3. www.incassomachtigen.nl
4. Payments Association, Annual Report 2015, www.betaalvereniging.nl
5. www.ideal.nl
6. www.idin.nl
7. Letter from the Minister of the Interior and Kingdom Relations to the Lower House, 21 December 2016

Cyber crime is becoming an ever greater part of the Public Prosecution Service's work. We believe that, within the next five years, roughly 50% of crime will have a digital component. In this context, criminal law, based of course on constitutional principles, will be used as an 'optimum remedium', or best possible solution for society, in conjunction with other forms of enforcement and surveillance. Criminal law can only be effective in a chain in which citizens, businesses and the government work together on prevention, awareness and willingness to invest in cyber security across the board.

Gerrit van der Burg
Member of the Board of the Procurators

WE MUST WORK TOGETHER AS PARTNERS IN A CHAIN

CYBER SECURITY MUST BE TAKEN FOR GRANTED

Photo: Frank Groeliken

Earlier this year, the appeal court in The Hague sentenced two men to long periods of imprisonment of 4.5 years and 45 months respectively. What offences had they committed? Computer crime, primarily manufacturing and deploying so-called web injects: malware that enables money to be stolen from online bank accounts. It is clear from this case that judges understand the seriousness of cyber crime. This wasn't just a lone hacker sitting in an attic who made a mistake. It involved crimes that could easily cause serious disruption to the whole of the online payment system. The perpetrators purchased off-the-shelf software online and adapted it to their needs: cybercrime-as-a-service, a trend that is becoming increasingly common. This case involved collaboration with partners in the ECTF, the partnership agreement between the police, the Public Prosecution Service and various financial institutions. This illustrates the need to work together as partners in a chain when fighting this form of cyber crime.

New cracks in firewall

The hack of the Democratic Party in the US has highlighted the issue of the security of data and systems. And, to my mind, rightly so. Criminals are constantly responding to and exploiting the latest technological developments. Phishing is

becoming ever more professional, more and more people are falling victim to ransomware and more and more small and medium-sized businesses are falling prey to Remote Access Trojans (RAT).
Advanced persistent threats threaten businesses and vital infrastructure. But new forms of cyber crime are also emerging. More and more devices are becoming semi-computers with their own connection to the Internet. Our alarm clock will soon be talking to our car so it is warmed up for us in the winter. Our refrigerator will be talking to the automatic supermarket delivery service. With every smart device in the Internet of Things we create a crack in our "firewall". Because every interaction with the outside world brings with it opportunities for hackers to penetrate the system and creates new challenges for detection.

Cybercrime-as-a-service

Another trend is the fact that it is becoming increasingly easy to commit cyber crime without any in-depth technical knowledge. You can buy your malware off the shelf for 50-150 dollars and use it to attack businesses and citizens at your leisure. DDoS attack providers advertise on YouTube. Just a few clicks of the mouse and it's sorted. Ransomware can be purchased on the Darkweb for 100 dollars. And there are hundreds of videos on YouTube on how to hack and how to prevent yourself from being caught. It goes without saying that these services will lead to an increase in hazardous cyber crime.

Cyber security is ever more important

The ease with which cyber crimes can be committed as a result of cybercrime-as-a-service makes cyber security ever more important. We take it for granted that children learn to swim and learn the rules of the road. But the teaching of cyber security is still in its infancy. When three-point seat belts first came in in 1959 people were skeptical about them. After all, a car is meant to represent freedom, so why would you want to be restricted by a seatbelt? Nowadays however, wearing a seatbelt in a car is no longer an issue. In my view, the same should apply to cyber security. It shouldn't feel odd, it should be something we take for granted. When you go online, you automatically wear your "digital seatbelt".

Duties of care

We must all strive for a situation whereby we ensure as a matter of course that our own individual cyber security or the cyber security of our organisation is effective and automatically spend time and money on this process. Ms Verhagen's report refers in this context to duties of care. Citizens, businesses and the government all have their own responsibility, both in respect of other businesses and in respect of consumers. After all, with the ever growing digitalisation of our society, poor cyber security can have significant consequences. Poor security can lead to commercial secrets and personal data being leaked through a hack or human error, for example, or can jeopardise a company's business continuity. In my view, these duties of care should also include companies that manufacture devices that are connected to the Internet. Secure software and regular updates can reduce the risk of cyber crime.
It is clear from the recent political and media attention around the inadequate security of government systems that poor cyber security is currently under the spotlight, and rightly so. There is a growing realisation that inadequate cyber security can damage confidence in the government's operations. Government institutions must act as role models when it comes to duties of care. This will however require significant investment.

Statutory powers

Criminals are increasingly using digital (encryption) technologies, services and tools to protect themselves from prosecution and to make detection more difficult. If detection is to be in a position to keep pace with today's cyber criminals, other prerequisites, such as adequate statutory powers, will be necessary.
It is therefore crucial for the Public Prosecution Service and the police that the Computer Crime Act III be adopted in order to make the detection and prosecution of cyber criminals easier. This act, which is commonly known, unfairly, as the 'hack act', gives detectives powers to detect serious criminal offences by intercepting suspects' communications before they are encrypted. The use of encryption and security techniques, which can be purchased cheaply online, hinders not only the fight against cyber crime but also efforts to tackle liquidations,

"Cyber crime is international: consequently investment in the harmonisation of international legislation and regulations is crucial."

Photo: Feije Riemersma - National Photo Bank

We take it for granted that children learn to swim and learn the rules of the road. But the teaching of cyber security is still in its infancy.

terrorism, child pornography, outlaw motorcycle gangs and drug crime.
Ransomware can be 'installed' by your neighbour but it can be installed just as easily by someone on the other side of the world. Cyber crime is international: it is not limited to a specific place or time. Consequently, investment in the harmonisation of international legislation and regulations is crucial.
Given the difficulty of tracking down international criminals, the growing use of encryption and the technical complexity of this issue, the Public Prosecution Service, together with its partners, is also focusing on improving its intelligence, increasing its knowledge and expertise and devising alternative interventions. By taking preventative or disruptive measures against cyber criminals, digital infrastructure or facilitators, cyber crime can be countered and damage prevented.

Criminal law as the best possible solution

Ms Verhagen's report recommends strengthening public-private partnerships in the field of cyber security. She also stresses the importance of education, duties of care and the raising of awareness. Together with its (international) partners, the Public Prosecution Service is working towards a situation in which society can rely on a secure digital environment and the Netherlands is unattractive to cyber criminals because it is clear that effective action is being taken to tackle cyber crime. Fighting cyber crime is not just the job of the Public Prosecution service and the police. Cyber security must be a priority for citizens, businesses and the government. Clearly, the 'core business' of the Public Prosecution Service is criminal law, but in the rapidly evolving field of cyber crime and cyber security, I see criminal law as an 'optimum remedium', in other words the best possible solution for society. Where detection and prosecution must be linked to other forms of enforcement and surveillance. Criminal law must be used to help make our digital society more secure and more resilient (always, of course, on the basis of constitutional principles). This requires collaboration, awareness, urgency and investment across the chain. Nationally and internationally.

The UK Government has set out its ambition and goals with regards to cyber security in the National Security Strategy (November 2015) and the National Cyber Security Strategy (NCSS) (November 2016). Our vision, as set out in the NCSS is that: the UK is secure and resilient to cyber threats, prosperous and confident in the digital world.

Nicholas J. Alexander
Cyber and Government Security Directorate
(author of the National Cyber Security Strategy 2016-2021)
Cabinet Office, UK

CYBER AS A TOP TIER ONE RISK TO UK INTERESTS

POLITICAL DIALOGUE AND UNDERSTANDING BETWEEN GOVERNMENTS IS KEY

This ambition reflects our determination to ensure we make the most of the opportunities that digitalisation affords our society and economy while ensuring that we do our utmost to manage and mitigate the associated risks and threats. The NCSS 2016-2021 is the second national strategy and is supported by £1.9 billion of transformational investment over five years. This investment contributes towards a range of measures including the establishment of the National Cyber Security Centre.

Vision

To realise the vision set out above we will work to achieve the following objectives:

- *Defend*
  We have the means to defend the UK against evolving cyber threats, to respond effectively to incidents, to ensure UK networks, data and systems are protected and resilient. Citizens, businesses and the public sector have the knowledge and ability to defend themselves.
- *Deter*
  The UK will be a hard target for all forms of aggression in cyberspace. We detect, understand, investigate and disrupt hostile action taken against us, pursuing and prosecuting offenders. We have the means to take offensive action in cyberspace, should we choose to do so.
- *Develop*
  We have an innovative, growing cyber security industry, underpinned by world-leading scientific research and development. We have a self-sustaining pipeline of talent providing the skills to meet our national needs across the public and private sectors. Our cutting-edge analysis and expertise will enable the UK to meet and overcome future threats and challenges.

Foto: Marco Govel - Hollandse Hoogte

The UK National Cyber Security Strategy 2016-2021 is the second national strategy and is supported by £1.9 billion of transformational investment over five years.

Investing in partnerships

Underpinning these objectives, we will pursue international action and exert our influence by investing in partnerships that shape the global evolution of cyberspace in a manner that advances our wider economic and security interests. By its very nature cyberspace is without borders. The UK is committed to working with all states to develop a common understanding in the benefits of a free, open, peaceful and secure cyberspace. This will involve building confidence and trust with all nations, maximising the mutual advantages that cyberspace has to offer while also enhancing our collective security online.

One of the key aspects of the strategy is the important role we identify for government. Good cyber security will always depend on cooperation between the citizen, industry and the state. But we believe that there is a particular and leading role for the Government to play. As we set out in the NCSS: 'The Government must set the pace in meeting the country's national cyber security needs. Only Government can draw on the intelligence and other assets required to defend the country from the most sophisticated threats. Only Government can drive cooperation across the public and private sectors and ensure information is shared between the two. Government has a leading role, in consultation with industry, in defining what good cyber security looks like and ensuring it is implemented'. But government cannot do this alone: everyone has role to play.

Risk to UK interests

The UK's 2015 National Security Strategy, reaffirmed cyber as a top tier one risk to UK interests – highlighting cyber threats as one of the key challenges to drive the UK security priorities for the coming decade. The scale and scope of the threat continues to evolve. The UK Government therefore drew up the Strategy and the Programme that 'will ensure that we have in place all the necessary components to defend the UK from cyber-attack. These include capabilities that allow us to understand and tackle the most advanced threats, law enforcement capabilities to deal with cyber crime, support for businesses particularly in the UK's CNI, and the skills and innovation needed for the long term'.

All governments make decisions on spending according to the priorities they set themselves. The UK Government, recognising the risk associated with cyber, decided it was appropriate to set aside a dedicated amount for trans-formational investment to increase our capacity across the public and private sector.

Criminal exploit

Digitalisation will continue to shape our economy and our society as new technologies come on stream or evolve. Unfortunately, the ingenuity of those who seek to exploit those technological developments for criminal purposes is likely to evolve just as rapidly. Exploitation of the Internet of Things has been such a technological evolution that some have sought to exploit for criminal ends. That said, there are also many governments, companies and gifted individuals who are working hard to protect us from those threats and thwart the criminals. While there will always be those who use the internet for criminal purposes, we can and will have the means to protect ourselves and bring those criminals to justice.

Opportunities

The greatest opportunities arise from the cooperation of governments and industry to afford greater protection to the citizen so that we can all go about our business online in safety and security. Some very clever minds are already doing some great work in this space, in a manner which could eventually change the balance of risk in favour of the individual, law-abiding citizen and against the criminal. Cooperation between governments remains an important opportunity. Better sharing of

information and technical understanding between national Computer Security Incident Response Teams (CSIRTs) is one way. Political dialogue and understanding between governments is also key, and we look forward to the meeting of the Global Conference on Cyberspace in India later this year to further this goal – the latest iteration in the process launched by the UK in 2011 and last held in The Hague in 2015. Raising global standards of cyber security through targeted capacity building work is another opportunity we will continue to pursue this year. The Global Forum on Cyber Expertise launched by the Dutch in 2015 provides an important platform for coordinating these efforts and I commend the leadership demonstrated by the Government of the Netherlands in this regard.

Tackle the threat

I know from personal experience, from having spent four years living in The Hague that the Netherlands is amongst the most advanced digital nations, with a robust National Cyber Security Strategy and structure of its own. In preparing for an eventual third Dutch NCSS, it will be worth considering where government and private sector skills and resources could be even better joined up to tackle the threat to the country's core interests.

Digital Golden Age

From my reading of the summary of the Verhagen report, there appear to be many features or issues raised which coincide with the UK and other similar national strategies. Advanced societies and economies like our own all share many of the same fundamental challenges in the field of cyber security – how to best protect ourselves while preserving and protecting individual rights and without stifling the innovation that is key to our digital futures. As noted above, one of the keys to success lie in a fruitful and cooperative relationship between the public and private sectors – something which I note features strongly in the report. The Netherlands, like the UK, is in many ways a digital leader, a major hub and centre of innovation, and an influential voice on cyber security. Maintaining and reinforcing cyber security will safeguard our future digital prosperity. Just as the Netherlands revolutionized global trade in the Golden Age, so I am confident that the Netherlands, by working closely with its oldest allies in the UK, will continue to set the pace of this Digital Golden Age.

> "Good cyber security will always depend on cooperation"

Foto: Hollandse Hoogte

Political dialogue and understanding between governments is also key.

Client: Dutch Cyber Security Council
Chief Editor: Elly van den Heuvel (secretary)
Concept and (final) editing: Martin Bobeldijk (Turnaround Communicatie)
With thanks to: Andrea Bakker, Martine Spaans and Siep van Sommeren
Photography: Arenda Oomen, Adriaan van Zijp, National Photo Bank and Hollandse Hoogte • **Illustrations:** Jasper Rietman
Layout and editing: BKB • **Printwork:** Xerox/OBT

March, 2017

CSR
Cyber
Security
Council