SPECIAL
EU EDITION

CSR MAGAZINE

Cyber Security Council
Cyber Security Raad

Cyber security provides a boost to the economy ◦ Protecting the EU institutions against cyber threats ◦ Our data shape who we are ◦ E-skills indispensable for a digital single market ◦ The Budapest Convention as a framework ◦ Important American developments for Europe

Year 2, No 2, January 2016

PREFACE

Nederland is in de eerste helft van 2016 voorzitter van de Europese Unie. De Cyber Security Raad (CSR) zal een actieve rol spelen tijdens dit voorzitterschap. Daarom staat deze tweede editie van het CSR Magazine geheel in het teken van Europa. Dit themanummer geeft inzicht in een aantal belangrijke ontwikkelingen op het gebied van cybersecurity. Verschillende Europese organisaties beschrijven hun visie op de digitale toekomst en de rol die zij spelen om Europa veilig en welvarend te houden.
Veel Europese landen werken op basis van een nationale cybersecurity strategie. De Europese Cyber Security Strategie (2013) en de binnenkort vast te stellen richtlijn voor Netwerk en Informatiebeveiliging (NIB) vormen een stevige basis voor een Europese cybersecurity aanpak. Echter, de technologische ontwikkelingen gaan snel. De komende jaren staat ons veel te wachten. Welke technologische ontwikkelingen zijn dat eigenlijk precies? En hoe bereiden we ons daar goed op voor? Welke rollen en verantwoordelijkheden horen daar bij voor lidstaten, burgers, organisaties? Deze strategische vraagstukken moeten een structurele basis krijgen in onze aanpak van cybersecurity. Niet alleen om ons goed te wapenen tegen de bedreigingen, maar vooral ook om de digitale economische kansen die ontstaan te kunnen benutten.
De CSR is een Nederlandse raad die binnen Europa samenwerkingsverbanden zoekt om strategische vraagstukken in gezamenlijkheid en vanuit een publiek privaat wetenschappelijk invalshoek te agenderen. De digitale uitdagingen gelden immers voor alle Europese landen. Wij onderschrijven het belang van een goede Europese samenwerking, zeker ook op strategisch niveau. Door bundeling van krachten kunnen we ons samen hard maken voor een vrij, open en economisch sterk Europa.

Namens de Cyber Security Raad
Eelco Blok, Dick Schoof

The Netherlands holds the presidency of the European Union for the first half of 2016. The Cyber Security Council (CSR) will play an active role during this presidency. That is why the second edition of the CSR Magazine is a special European edition. This themed edition provides an insight into a number of important developments with respect to cyber security. Various European organisations have defined their vision of the digital future and the role that they play in order to keep Europe safe and secure.
Many European countries are working on the basis of a national cyber security strategy. The European Cyber Security Strategy (2013) and the guideline for Network and Information Security (NIB) that is soon to be drafted, form a robust basis for a European cyber security approach. However, technological developments evolve very quickly. We will be faced with many issues in the years to come. What technological developments are these, exactly? And how can we prepare ourselves for them? What roles and responsibilities correspond to Member States, citizens and organisations? We must create a structural basis for these strategic issues within our approach to cyber security. Not only to arm us effectively against threats, but also to effectively use the digital economic opportunities that are created.
The CSR is a Dutch Council which seeks to put strategic issues collectively and from a public/private scientific perspective, on the agenda within the European cooperative partnerships. The digital challenges apply to all European countries. We stress the importance of good European cooperation, especially on a strategic level. The combination of forces will enables us to collectively defend a free, open and economically strong Europe.

On behalf of the Cyber Security Council
Eelco Blok, Dick Schoof

INHOUD CONTENTS

CSR Cyber Security Council | Cyber Security Raad

Rijksoverheid/Arenda Oomen

Digitalisering biedt enorme kansen: voor persoonlijke en maatschappelijke ontwikkeling, voor het bedrijfsleven, de economie en dus ook voor onze welvaart. “Maar dan zullen we wel voortdurend alert moeten zijn én blijven op de veiligheid van het digitale domein”, zegt staatssecretaris Klaas Dijkhoff. “Goede cybersecurity is van cruciaal belang om welvaart vast te houden.” Tijdens het EU-voorzitterschap in de eerste helft van 2016 besteedt Nederland daarom uitgebreid aandacht aan dit onderwerp. *Digitisation creates massive opportunities: for our personal and societal development, for enterprise, for the economy and, thus, for our prosperity. “But we do need to constantly be and remain mindful of the security of the digital domain,” State Secretary Klaas Dijkhoff explains. “Sound cyber security is of the essence if we are to retain our prosperity.” The Netherlands are therefore set to use their EU presidency during the first six months of 2016 to extensively draw attention to the topic.*

STAATSSECRETARIS VEILIGHEID EN JUSTITIE, KLAAS DIJKHOFF:

The State Secretary of Security and Justice, Klaas Dijkhoff:

‘CYBER SECURITY PROVIDES A BOOST TO THE ECONOMY’

Dijkhoff is gedreven als het aankomt op het creëren en behouden van veiligheid en vrijheid. Beide horen volgens hem bij elkaar. “Zonder veiligheid geen vrijheid en daardoor ook geen creativiteit en ruimte om iets moois te laten ontstaan tussen mensen.” Om die reden zet hij zich in om criminelen de pas af te snijden voor maatregelen om cyberincidenten te voorkomen. Cybersecurity is dan ook een thema dat hem aan het hart ligt. “Gewone burgers en het midden- en kleinbedrijf hebben last van cybercriminelen. Dat geldt natuurlijk ook voor grotere bedrijven en de vitale sectoren in Nederland. Uit het Cybersecurity Beeld Nederland 2015 blijkt dat allerlei vormen van fraude hen parten spelen. Het zijn vaak oude, bekende trucjes, maar nu in een nieuw, digitaal jasje. Daarnaast blijft digitale spionage en diefstal van intellectueel eigendom een belangrijke dreiging voor het bedrijfsleven.

Dijkhoff is a driven man when it comes to creating and safeguarding security and freedom. He believes the two concepts are inherently connected. “Without security, there can be no freedom and, thus, no creativity and room for people to build something together.” He is committed to counter criminals by implementing measures to prevent cyber incidents. Cyber security is a topic that is dear to his heart. “The activities of cyber criminals affect both citizens and enterprises, including larger corporations and those active in sectors vital to the Dutch economy. As becomes evident from the Netherland’s 2015 Cyber Security Assessment, many are affected by fraud in its many guises. Often, criminals employ old and well-known tricks, albeit in a new, digital dress. In addition, digital espionage and theft of intellectual property remain significant threats to the business sector. Effective cyber security measures are required to reduce cybercrime.”

What are your cyber security ambitions for the EU presidency?

“First and foremost, it should be understood that we will not focus on implementing new rules. Let’s first make sure that the existing ones are properly implemented. In every Member State, that is. For the level of cyber security still differs greatly from one EU State to the next. It would be great if we could use the Dutch presidency term to make significant headway with implementing the EU Cyber Security Strategy. Proper implementation is only possible if all relevant partners - public, private and academic - cooperate intensively. I believe that our Dutch Cyber Security Council, which is composed of public, private and academic partners, could serve as an example to the rest of the EU on issues like raising awareness, actively sharing knowledge and learning from each other. Especially in case of incidents or emergencies.

OM DREIGINGEN EFFECTIEF HET HOOFD TE KUNNEN BIEDEN, ZULLEN WE MOETEN KOMEN TOT EEN INTERNATIONAAL NETWERK VAN SAMENWERKENDE CERT'S

TO COUNTERACT THREATHS EFFECTIVELY, WE HAVE TO DEVELOP AN INTERNATIONAL NETWORK OF COOPERATING CERT'S

Goede cybersecuritymaatregelen gelden daarbij als voorwaarde voor het verminderen van cybercrime."

Wat zijn uw ambities op het terrein van cybersecurity tijdens het EU-voorzitterschap?

"Laat ik vooropstellen dat we ons niet gaan richten op nieuwe regels. Laten we ons eerst maar eens richten op een goede uitvoering. In alle lidstaten, want het niveau van cybersecurity in de verschillende EU-landen loopt nog sterk uiteen. Het zou mooi zijn als we tijdens het Nederlandse voorzitterschap de implementatie van de EU Cyber Security Strategie een stuk verder kunnen brengen. Een goede uitvoering kan alleen van de grond komen als er sprake is van intensief samen optrekken van alle relevante partners: publiek, privaat én vanuit de wetenschappelijke hoek. Ik denk dat onze Nederlandse Cyber Security Raad, met zijn publiek-privaat-wetenschappelijke samenstelling, op dit punt als goed voorbeeld kan dienen binnen de EU. Bijvoorbeeld als het gaat om awareness vergroten, actief kennis delen en van elkaar leren. Zeker ook in geval van incidenten en calamiteiten. Melding daarvan, in een vroeg stadium, is van cruciaal belang. Dat draagt ertoe bij dat we problemen effectiever kunnen aanpakken."

Waarom is een belangrijk doel van het voorzitterschap om Computer Emergency Response Teams (CERT's) in te richten in de lidstaten?

"In de Nederlandse CERT (Nationaal Cyber security Center) komen publieke en private partijen bij elkaar om gezamenlijk cyberdreigingen te bekijken en te beoordelen. En om snel en passend te reageren in geval van incidenten en calamiteiten. U weet, digitale dreigingen trekken zich niks aan van landsgrenzen. Om dreigingen effectief het hoofd te kunnen bieden, zullen we dus moeten komen tot een internationaal netwerk van goed samenwerkende CERT's. Als Nederland zijn wij zeker bereid om andere landen te helpen met het inrichten van een eigen CERT."

Die publiek-private samenwerking heeft Nederland al een mooie 'best practice' opgeleverd: responsible disclosure. Gaat u dit presenteren aan andere EU-lidstaten?

"Ja, waar het gaat om samenwerking tussen hackers, overheden en bedrijven is Nederland echt koploper. Op basis van richtlijnen voor responsible disclosure melden ethische hackers op een verantwoorde manier kwetsbaarheden in ICT-systemen. Dat helpt de betreffende organisaties om die kwetsbaarheden aan te pakken en uit te bannen. Dat vergt groot vertrouwen, van alle partijen. We zijn er als Nederland best trots op dat we deze situatie hebben weten te bereiken. "

Een ander groot thema is de EU-richtlijn over netwerk- en informatiebeveiliging, de NIB-richtlijn. Wat is het belang hiervan en wanneer wordt deze ingevoerd?

"Die richtlijn is van groot belang. Ze regelt voor alle lidstaten de inrichting van nationale structuren op het terrein van cybersecurity. Je kunt je voorstellen dat implementatie van die richtlijn een enorme stimulans betekent voor de internationale samenwerking op het gebied van cybersecurity. We hopen de richtlijn tijdens het Nederlands voorzitterschap te kunnen vaststellen, zodat alle landen snel kunnen beginnen met de implementatie."

It is vital that such situations are reported as early as possible, as it would help us to tackle problems more effectively."

Why is the establishment of Computer Emergency Response Teams (CERTs) in the Member States such an important presidency objective?

"The Dutch CERT, the National Cyber Security Centre, brings public and private parties together to jointly inspect and assess cyber threats, and to respond both quickly and effectively should an incident or emergency occur. As you know, digital threats do not stop at the border. This means that, to effectively respond to any threat, we need to establish an international network of closely cooperating CERTs. The Netherlands is ready and willing to help other countries in establishing their own CERT."

This public-private partnership has already given the Netherlands a solid 'best practice': responsible disclosure. Do you intend to present it to the other EU Member States?

"Absolutely, in terms of the close cooperation between the IT Community, governments and businesses, the Netherlands is a frontrunner. Our responsible disclosure guidelines stipulates that ethical hackers report on IT systems vulnerabilities in a responsible manner. This helps the organisations affected to get to work and remove those vulnerabilities. This requires a lot of trust, from all parties concerned. As a country, we're pretty proud of having achieved this. "

Another important topic is the EU Network and Information Security Directive, or the NIS Directive. Why is it so important, and when will it be implemented?

"This Directive is of the utmost importance. It lays down the organisation of national cyber security structures for all Member States. As you can surely imagine, the implementation of this Directive would provide a massive boost to international cyber security cooperation. Our aim is to adopt the Directive during the Dutch EU presidency term, allowing all countries to quickly proceed with implementing it."

In what other ways can European cyber security cooperation be improved?

"In many. The development of standards, secure hardware and software, and methods for the teaching of secure coding,

Op welke andere terreinen kan de Europese samenwerking op het terrein van cybersecurity nog worden verbeterd?

"Vele. Denk bijvoorbeeld aan de ontwikkeling van standaarden, veilige hard- en software en onderwijsmethodieken voor veilig programmeren. In Nederland kennen we al zo'n methodiek, ontwikkeld door de Secure Software Foundation. Ook die willen we binnen de EU breder onder de aandacht brengen. Je ziet: cybersecurity wordt ook steeds meer een economisch item. We leren van elkaar, komen zo tot een steeds veiliger digitaal domein en geven tegelijkertijd ook de economie een mooie stimulans. Doordat Nederland een van de landen is die voorop loopt in digitalisering, krijgen we als eerste klappen uitgedeeld. Vervelend. Maar het is ook een kans. Het geeft ons de gelegenheid om een remedie te ontwikkelen tegen deze aanvallen. Ons bedrijfsleven is daardoor in staat wereldwijd te helpen bij het verbeteren van cybersecurity. Zo wordt cybersecurity voor Nederland een exportproduct."

Is 'the Dutch approach' een voorbeeld voor andere EU-lidstaten?

"Ik denk zeker dat andere landen met veel belangstelling naar onze aanpak kijken. Het is mooi dat die oeroude, nuchtere Hollandse aanpak van 'polderen' ook binnen het 'gloednieuwe' cyberdomein blijkt te werken. Onze aanpak wordt gekenmerkt door publieke, private en wetenschappelijke stakeholders met een totaal verschillende achtergrond, die over de schotten heen durven kijken en de samenwerking zoeken. Uit een welbegrepen eigenbelang, maar daardoor ook in het algemeen belang van Nederland en Europa. Met de Cyber Security Raad als drijvende kracht, de Nationale Cyber Security Strategie als wegenkaart en het jaarlijkse Cyber Security Beeld als 'actuele verkeersinformatie' zijn we in staat adequaat richting te geven aan onze cyberaanpak en waar nodig telkens onze koers bij te stellen. Dit model zal mogelijk niet voor alle landen werken, maar wie er voor openstaat, nodig ik van harte uit om eens een kijkje in onze keuken te nemen."

---

for instance. We already have such a method in place in the Netherlands, developed by the Secure Software Foundation. We aim to raise wider EU awareness. As you can see, cyber security is also becoming more of an economic issue. We learn from one another, create a more secure digital domain, and at the same time, provide a nice boost to the economy. As the Netherlands is a forerunner in digitisation, we are one of the first countries to encounter its adverse effects. Troublesome, to be sure. But it's also an opportunity. For it allows us to develop remedies to counter such attacks. This allows Dutch businesses to become globally active in improving cyber security, turning it into a Dutch export product."

Does the 'Dutch approach' serve as an example for the other EU Member States?

"I do believe other countries are very interested in what we do. It's great to see that our sensible, quintessentially Dutch approach of seeking consensus still works in the 'brand-new' cyber domain. Our approach is characterised by public, private and academic stakeholders, each coming from a totally different background, daring to look beyond their own worlds and seeking out collaboration. For reasons of self-interest, to be sure, but in so doing they also act in the general interest of the Netherlands and Europe. By having Cyber Security Council as our driving force, the National Cyber Security Strategy as a roadmap and the annual Cyber Security Assessment as an overview of where we are at, we're able to effectively steer our cyber approach and change course whenever necessary. Though I admit this model might not be suitable for all countries, I cordially invite everyone interested to come and have a look behind the scenes."

MEMBERS OF THE CYBER SECURITY COUNCIL

DE LEDEN VAN DE CYBER SECURITY RAAD

PRIVATE SECTOR


Mark Engelen

Dhr. drs. E. Blok (co-voorzitter/*co-chairman*) – Voorzitter Raad van Bestuur en CEO van KPN, lid van CSR namens VNO-NCW, de grootste ondernemersorganisatie van Nederland • *Chairman of Board of Directors and CEO of KPN, member of CSR on behalf of VNO-NCW, the Confederation of the Netherlands Industry and Employers (known as VNO-NCW) is the largest employers' organization in the Netherlands*


Mark Engelen

Dhr. B. Hogendoorn – CEO Hewlett Packerd Nederland, lid van CSR namens Nederland ICT, de branche-organisatie van de Nederlandse ICT-sector • *(CEO Hewlett Packerd Netherlands), member of CSR on behalf of Nederland ICT, the trade association of the Dutch ICT sector*


Miranda Koopman

Dhr. M. Krom – CIO PostNL, lid van CSR namens CIO Platform Nederland, de vereniging voor digitalisering en/of ICT in private en publieke organisaties in Nederland • *CIO PostNL, member of CSR on behalf of CIO Platform Netherlands, the Dutch association for digitalisation and/or ICT in private and public organizations in the Netherlands*


Peter van ES

Mw. T. Netelenbos – Voorzitter ECP, lid van CSR namens ECP Platform voor de Informatiesamenleving, een neutraal platform van bedrijfsleven, overheid en maatschappelijke organisaties en heeft tot doel het gebruik van ICT in de Nederlandse samenleving te versterken • *Chairman of the ECP, member of CSR on behalf of ECP Platform of the information society, an independant platform of industry, government and civil society organizations The ECP goal is to enforce the use of ICT in Dutch Society*

PUBLIC SECTOR


Mark Engelen

Dhr. drs. H.W.M. Schoof (co-voorzitter/*co-chairman*) – Nationaal Coördinator Terrorisme-bestrijding en Veiligheid • *National Coordinator for Security and Counterterrorism*


Lenny Oosterwijk

Dhr. Mr. R.A.C. Bertholee – Directeur-Generaal Algemene Inlichtingen- en Veiligheidsdienst (AIVD) • *Director-General of the AIVD (Dutch Intelligence Service)*


Mark Engelen

Dhr. Mr. G.W. Van der Burg – Lid van het College van procureurs-generaal, lid van CSR namens Openbaar Ministerie • *Member of Board of Public Prosecuters, member of CSR on behalf of the Public Prosecution Service*


Rijksoverheid

Dhr. drs. M.E.P. Dierikx - Directeur-generaal Energie, Telecom en Mededinging bij het ministerie van Economische Zaken • *Director-General of Energy, Telecom and Competition at the Ministry of Economic Affairs*

ACADEMIC SECTOR


Miranda Koopman

Mw. Dr. B. Van den Berg - Hoofddocent eLaw Universiteit Leiden, eLaw - Centrum voor recht en digitale technologie onderzoekt de rol van recht in de informatiemaatschappij • *Professor of eLaw Leiden University eLaw - The Center for Law and Digital Technologies researches the role of law and regulation in the information society*


Mark Engelen

Dhr. Prof. Dr. M.J.G. Van Eeten – Hoogleraar Bestuurskunde Technische Universiteit Delft • *Professor of Public Administration at Delft University of Technology*


Mark Engelen

Dhr. Prof. Dr. B.P.F. Jacobs – Hoogleraar Computerbeveiliging Radboud Universiteit Nijmegen • *Professor of Digital Security at Radboud University Nijmegen*


Miranda Koopman

Mw. Prof. mr. E.M.L. Moerel - Senior Of Counsel Morrison & Foerster LLP, Hoogleraar Global ICT Law Universiteit Tilburg • *Senior of Counsel Morrison & Foerster LLP, Professor Global ICT law at Tilburg University*


Miranda Koopman

Dhr. J. Nijhuis – CEO Schiphol Group, lid van CSR namens sector vervoer • *CEO Schiphol Group), member of CSR on behalf of the transport sector*


Mark Engelen

Dhr. Ir. B.G.M. Voorhorst – COO TenneT, lid van CSR namens de Vitale Infrastructuur • *COO TenneT, member of CSR on behalf of the Critical Infrastructure*


Mark Engelen

Dhr. D.G.T.M. Heerschop – CIO Nationale Politie • CIO National Police


Miranda Koopman

Dhr. Dr. S.J.G. Reyn – directeur Strategie, Beleidsontwikkeling en Innovatie, lid van CSR namens Ministerie van Defensie • *Director Strategy, policy-making and innovation, member of CSR on behalf of the Ministry of Defence*


Mark Engelen

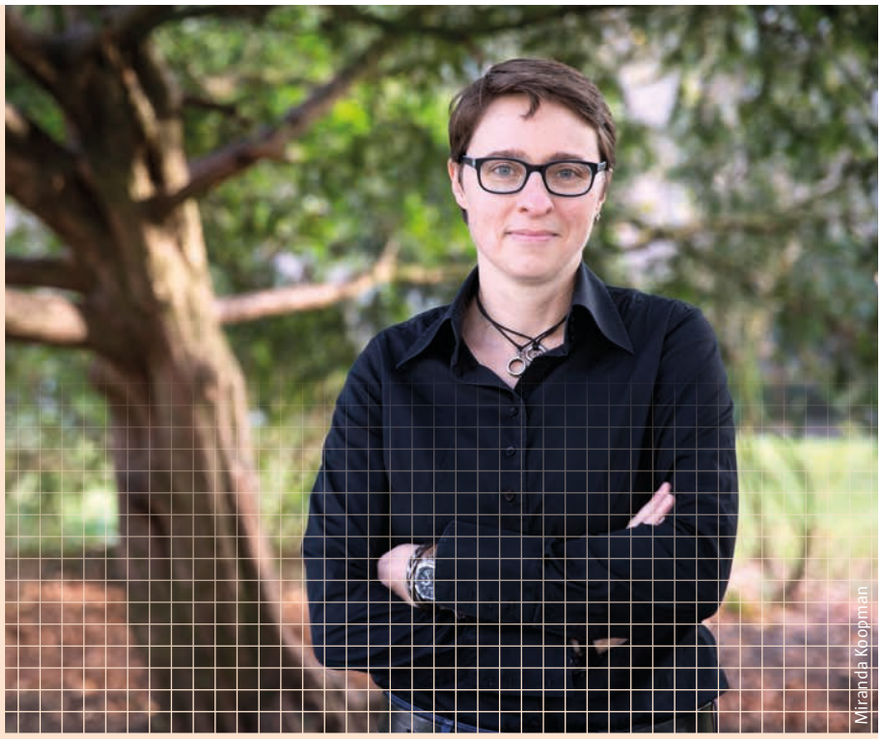
Dhr. drs. H.B. Eenhoorn – Digicommissaris. De Digicommissaris is door het Kabinet aangesteld om, als overheidsbrede regisseur, een programma op te stellen dat is gericht op het leggen van een overheidsbrede infrastructurele basis voor een digitale overheid, voor nu en in de toekomst • *Digicommissaris. The 'Digicommissaris' is appointed by the Cabinet as director of the digital government*


Miranda Koopman

Mw. Drs. E.C. Van den Heuvel
Secretaris • *Secretary of the Council*

BIBI VAN DEN BERG

new member of the Cyber Security Council



‘IT IS TIME FOR A SOCIAL DEBATE’

Bibi van den Berg is sinds 2012 als hoofddocent verbonden aan eLaw, Centrum voor Recht en Digitale Technologie binnen de Faculteit Rechtsgeleerdheid van Universiteit Leiden. Ze heeft de leiding over de Cybersecurity Governance groep van het Institute for Security and Global Affairs aan de Campus Den Haag van dezelfde universiteit en is één van de trekkers van de Cyber Security Academy. *Bibi van den Berg has been a senior lecturer in eLaw, Centre for Law and Digital Technology at the Faculty of Law of the University of Leiden, since 2012. She is in charge of the Cybersecurity Governance Group of the Institute for Security and Global Affairs at the Hague Campus of the same university and is one of the initiators of the Cyber Security Academy.*

Cybersecurity en het Internet der Dingen zijn ‘hot topics’. Weten mensen eigenlijk wel hoe deze thema’s hun leven beïnvloeden?

“Er is veel onduidelijk over deze materie bij het grote publiek. Mensen willen graag meer weten over deze ontwikkelingen, maar kunnen feiten en ‘broodje aap verhalen’ moeilijk van elkaar scheiden. Daarom wordt het tijd voor een maatschappelijk debat over deze onderwerpen. Zodat burgers weten wat er speelt, welke risico’s zij lopen, wat ze daartegen kunnen doen en welke afwegingen zij kunnen maken. Ik wil daar vanuit mijn wetenschappelijke achtergrond graag aan bijdragen.”

Wat is de reden dat u bent toegetreden tot de Cyber Security Raad (CSR)?

“Door deelname aan de CSR kan ik als wetenschapper zaken die ik uitdenk vertalen naar een beleidsrelevante context. Op die manier draag ik bij aan de invloed die de raad heeft op de cybersecurity-strategie en het cybersecurity-beleid in Nederland. De raad is een publiek-privaat-wetenschappelijk orgaan dat op strategisch niveau adviseert en indien nodig een tegenstem laat horen. Ieder land zou zo’n onafhankelijk en strategische adviesorgaan moeten hebben om cybersecurity nationaal op de agenda te zetten en te houden.”te maken heeft met de kern van wat je doet.”

Cyber security and the Internet of Things are ‘hot topics’. Do people actually know how these topics affect their life?

“The general public does not understand much about these issues. People would like to know more about these developments, but find it difficult to distinguish between facts and nonsense. This is why it is time for a social debate about these issues, so that citizens know what is happening, what the risks are, what they can do against them and what considerations play a role. I would like to contribute to this debate from my own scientific background.”

What is the reason that you joined the Cyber Security Council (CSR)?

“By participating in the CSR I, as a scientist, can place issues that I reflect about in a policy-relevant context. In this way I can contribute to the influence the Council has on the cyber security strategy and cyber security policy in the Netherlands. The Council is a public-private-scientific body that advises on a strategic level and, if necessary, has a dissenting voice. All countries should have such an independent and strategic advisory body to place and keep cyber security on the national agenda.”

With **Bibi van den Berg**, Professor eLaw Leiden University

"Waarom moet alles aan het internet hangen?" Die vraag stelt Bibi van den Berg, hoofddocent eLaw aan de Universiteit Leiden, zichzelf regelmatig. Zij is gespecialiseerd in het Internet der Dingen. "In het Internet der Dingen zijn apparaten zoals koelkasten, auto's, en thermostaten via het internet met elkaar verbonden. Die ontwikkeling zet zich voort. Het is maar zeer de vraag of de samenleving begrijpt welke consequenties dat heeft." *"Why should the internet be used for everything?" Bibi van den Berg, associate professor at eLaw, the Center for Law and Digital Technologies at Leiden University, often wonders about this question. She specialises in the Internet of Things. "The emergence of the Internet of Things means that objects such as fridges, cars, and thermostats are connected with each other through the internet. This development is on the rise. It is doubtful whether society realises what consequences this has."*

IN OUR SOCIETY THERE IS LESS PRIVACY

'OUR DATA SHAPE WHO WE ARE'

Het Internet der Dingen biedt volgens Van den Berg enorm veel mogelijkheden. Zij verwacht dat veel zaken in de toekomst makkelijker en beter zullen gaan. "Denk aan het optimaliseren van productieprocessen, het oplossen van milieu- en energieproblemen en het innoveren van de gezondheidszorg."

Dat lijkt allemaal positief. Kleven er ook nadelen aan het 'Internet of Things'?

"De keerzijde is dat we een stuk privacy inleveren. En daar zijn we ons vaak niet eens van bewust. Waarom moet alles eigenlijk aan het internet hangen? Vroeger gingen de dingen ook goed. Waarom moet de oven van de bakker op de hoek aan het internet hangen, zodat hij via zijn

According to Van den Berg, the Internet of Things offers many opportunities. She expects that networked technologies will provide increased efficiency and convenience in many sectors of society in the future. "Examples include the optimisation of production processes, or tackling environmental and energy problems and innovating the health care."

All this seems very positive. Are there disadvantages with regard to the Internet of Things?

"One downside is that we lose a certain degree of privacy. And we are often not aware of this. Why should we actually use the internet for everything? In the past things worked well enough. Why should the oven of the baker on the corner be connected to the internet, so that he can read on his mobile phone when his rolls are ready? What is the added value there, except perhaps a better night's rest than before? Does the baker know that he is making himself very vulnerable and that he is giving away a lot of data in the process? Another example. There is a health app on your phone which individuals can use to check their health on a daily basis. But do they know who has access to their health data, and what happens with it? Samsung or Apple may sell these data, or use them to create profiles, which can be sold to health insurers or financial institutions. This may affect the level of the premium of individuals' health insurance, or whether or not they are accepted for a mortgage. Imagine that their data show that they have an increased risk profile. Will individuals still

Mausbaus

WE HEBBEN GEEN CONTROLE MEER OVER DE BIG DATA

WE ARE NO LONGER IN CONTROL OF BIG DATA

gsm kan lezen dat zijn broodjes klaar zijn? Wat levert dat op, behalve iets meer nachtrust dan voorheen? Weet de bakker wel dat hij zichzelf hier erg kwetsbaar mee maakt en heel veel persoonlijke gegevens zomaar weggeeft?
Nog een voorbeeld. Op je telefoon zit een gezondheidsapp. Als je die gaat gebruiken om te meten hoe het dagelijks met je gezondheid gesteld is, kan dat geruststellend zijn. Maar weet je wat er gebeurt met de data die je vrijwillig weggeeft? Samsung of Apple verkopen die data, er worden profielen mee gemaakt en die kunnen worden verkocht aan zorgverzekeraars of financiële instellingen. Dat kan van invloed zijn op de hoogte van de premie van je ziektekostenverzekering, of de hypotheek die je krijgt. Want stel dat uit jouw data blijkt dat je een verhoogd risicoprofiel hebt? Ben je dan nog steeds blij met je gezondheidsapp?
Het gevaar van dit soort 'makkelijke' hulpmiddelen is dat ze niet transparant zijn en dat we geen controle meer hebben over de big data die gaan bepalen wie we zijn."

Wat kan de argeloze burger hiertegen doen?
"Je kan gebruik maken van hulptools zoals blockers die je zoekgegevens in zoekmachines blokkeren of anonimiseringstools. Je kan met verschillende pc's werken en aliassen gebruiken. Maar dat vereist 'awareness'. De burger moet zich ervan bewust zijn wat er kan gebeuren met zijn data. Hij moet een weging kunnen maken tussen het inleveren van privacy en het opleveren van gemak."

Wat is de taak van de overheid en van het bedrijfsleven hierin?
"Overheid en bedrijfsleven moeten dit soort risico's deels inzichtelijker maken en deels wegnemen voor de burger. Vergelijk het met het wegenstelsel. Dat wordt door de overheid aangelegd, in samenwerking met de private sector. De infrastructuur, de borden boven de weg en de verkeersregels worden voor de burger gemaakt. Daardoor is een basale vorm van veiligheid op en rondom de weg gewaarborgd. De eigen inbreng van de burger is zorgen voor veilig gedrag op

be happy with their health app if using it might have serious (financial) consequences in the real world?
The risk of this type of 'easy' tools is that they are not transparent and that we are not in control anymore of the big data that shape who we are."

What can unsuspecting citizens do against this?
"They can use tools such as blockers that block their search data in search engines or anonymization tools. They can work with different pcs and user aliases. However, this requires 'awareness'. Citizens must be aware of what can happen with their data. They must consider the advantages and disadvantages of the intrusion of their privacy and weigh this against the convenience of certain 'easy' tools."

What is the task of the government and businesses in this?
"Governments and businesses play a role in making these types of risks more transparent for citizens. They can also play a role in (partially) removing them. One could compare it with the road system. This is built by the government, in cooperation with the private sector. The infrastructure, the signs above the roads and the traffic rules are made for citizens. This guarantees a basic form of safety on and around the roads. Citizens also contribute to road safety. They do so through safe driving behaviour, which is explicated by having a driving licence, knowing the rules and observing them. There is a parallel here with the digital motorway. Having said that, partially this issue is also a matter

ONTWIKKEL MEER TOLERANTIE VOOR ONVEILIGHEID

DEVELOP A GREATER TOLERANCE FOR INSECURITY

de weg, bijvoorbeeld door het hebben van een rijbewijs, kennis van de regels en het volgen van die regels. Die analogie zou je moeten doortrekken naar de digitale snelweg. Maar het is ook een kwestie van wennen aan de veranderende maatschappij. We krijgen een samenleving waarin veel meer gegevens op straat liggen. Een wereld die onveiliger is. Een van de oplossingen is dat we meer tolerantie voor onveiligheid ontwikkelen."

Welke kansen ontstaan door het Internet der Dingen?

"Zolang het Internet der Dingen de privacy van mensen niet raakt, is het een prachtige ontwikkeling. Bijvoorbeeld op het vlak van infrastructuur en industrie. Nederland is een land dat vooroploopt in dijkbewaking en kennis daarover. Met het Internet der Dingen kan dijkbewaking op een nog hoger niveau gebracht worden. Daarmee kunnen we echt een voorbeeld worden voor andere landen. Ook in hoogwaardige en intensieve landbouw kan het Internet der Dingen een voordeel zijn en kan Nederland scoren. Ik zie dan ook zeker kansen voor onze economie, welvaart en export."

Wat is de rol van de Cyber Security Raad?

"De raad heeft als taak het onderwerp op de maatschappelijke agenda te zetten en kan een leidende rol op zich nemen in het maatschappelijk debat. Het is immers een onafhankelijke raad die op strategisch niveau advies kan geven en zo nodig een tegenstem kan laten horen. Publieke, private en wetenschappelijke partijen hebben vaak andere belangen, maar de CSR stelt zich a-politiek op en staat boven de belangen. Daardoor kan de raad discussies losmaken en met gewogen oplossingsrichtingen komen."

of getting used to a changing society. We will have a society with less privacy, where much of our personal details can be used elsewhere. It will be a less secure world. One of the solutions is that we develop a greater tolerance for insecurity."

What are opportunities created by the Internet of Things?

"As long as the Internet of Things does not affect the privacy of people, it is a fantastic development. For example in the field of infrastructure and industry. The Netherlands is a country that is ahead in water management and has advanced knowledge about this issue. With the Internet of Things it is possible to improve water management even more. By doing this, we can be a real example for other countries. The Internet of Things may also be an advantage for high-quality and intensive agriculture. The Netherlands may score with this. I therefore certainly see opportunities for our economy, prosperity and export."

What is the role of the Cyber Security Council?

"The task of the Council is to place the issue on the societal agenda and have a leading role in the societal debate. After all, it is an independent council which can offer advice at a strategic level and, if necessary, have a dissenting voice. Public, private and scientific parties often have different interests, but the CSR is apolitical and is above the interests of parties. This means that the Council can initiate discussions and come up with deliberated problem-solving approaches."


Miranda Koopman

‘PUBLIC-PRIVATE PARTNERSHIP IS A MUST’

JOS NIJHUIS

new member of the Cyber Security Council

Jos Nijhuis is sinds 2009 president en CEO van de Schiphol Group. Hij bekleedt daarnaast verschillende nevenfuncties, onder andere als commissaris bij de SNS Bank en Aon Groep Nederland B.V.. In 2015 is hij toegetreden tot de Cyber Security Raad (CSR). *Jos Nijhuis has been serving as CEO of Schiphol Group since 2009. In addition, he holds various ancillary positions, like that of supervisory director at SNS Bank and Aon Groep Nederland B.V. In 2015, he joined the Cyber Security Council.*

Schiphol is een internationaal hooggewaardeerde luchthaven. Tientallen miljoenen passagiers komen en gaan. Op welke wijze speelt technologie een rol in het contact met de reiziger?

“Al onze processen worden ondersteund door ICT. Onze ambitie is om dit verder uit te bouwen en de beste digitale luchthaven van de wereld te worden. In al onze processen willen we het hoogste technologieniveau integreren en de klant van huis tot vliegtuig digitaal ontzorgen. Een voorbeeld hiervan is het waarschuwen van een reiziger als hij te laat dreigt aan te komen bij zijn vliegtuig, terwijl zijn bagage al aan boord is. Als de reiziger met ons deelt waar hij zich bevindt, krijgt hij een melding dat hij met spoed naar de gate moet gaan.”

Wat is de reden dat u bent toegetreden tot de Cyber Security Raad?

“Ik geloof in de meerwaarde van publiek-private samenwerking en kennisuitwisseling op het gebied van cybersecurity, binnen de luchtvaart en over sectoren heen. Systemen zijn dermate afhankelijk van elkaar dat samenwerken een must is. Daarnaast zet ik mij graag in voor bewustwording over digitale veiligheid, zodat mensen goed begrijpen welke kansen en risico’s er zijn. Ik zie de CSR als een urgentieplatform, dat onafhankelijk belangrijke strategische onderwerpen onder de aandacht brengt, zowel nationaal als internationaal. De CSR is echter geen vrijblijvend adviesorgaan. Overheid en bedrijfsleven moeten met onze adviezen aan de slag. Daar draag ik graag aan bij.”

Amsterdam Airport Schiphol is a highly regarded airport internationally. Annually, it services tens of millions of passengers. What role does technology play in the contact with the passenger?
“All our processes are supported by IT. Our ambition is to continue digitising and to become the world’s best digital airport. Our aim is to integrate the highest level of technology in all our processes and to use digital processes to remove all passenger worries, from the moment they leave their homes until the moment they enter their plane. One example would be issuing a warning to a passenger if he is in danger of being too late to arrive at the gate while his baggage is already on board. If the passenger shares his location, he will receive a notification urging him to proceed to the gate as quickly as possible.”

Why did you become a member of the Cyber Security Council (CSC)?
I believe in the added value of public private partnerships and exchange of knowledge in the field of cyber security, both in the aviation industry and in all related sectors. Systems are so interdependent that cooperation is a must. In addition, I like to work on raising awareness on digital security and on ensuring that people are well aware of all opportunities and risks. I consider the CSC to be an emergency platform that independently puts a spotlight on strategic topics, both on the national and the international level. The CSC recommendations are not free of obligation, however. Governments and businesses do need to “get to work” implementing our advice. And I am happy to contribute wherever I can.”

By **Nicolas Castellon**,
Cyber Security Researcher
Specializing in Critical Infrastructure
Protection and Big Data.

Cyberspace is de volgende uitdaging voor governance. Dit domein is een steunpilaar geworden voor het functioneren van de moderne maatschappij en bestaat momenteel uit zo'n 4,88 miljard verbonden apparaten en circa 7,9 zettabyte (een biljoen gigabyte) aan data en content. *Cyberspace is the next frontier for governance. This domain has a become a cornerstone for the functioning of modern society, currently consisting of roughly 4.88 billion connected devices and about 7.9 Zettabytes (one trillion Gigabytes) of data and content.*

CYBER SECURITY GOVERNANCE: SECURING CYBERSPACE

Schattingen tonen aan dat het aantal aangesloten apparaten in 2020 zal stijgen naar 25 biljoen, en het aantal geproduceerde data 35 Zettabytes zal bereiken. Deze aantallen indiceren dat meer analoge apparaten digitaal verbonden zullen worden en gaan communiceren via cyberspace, waardoor we nog meer met elkaar verbonden zullen zijn.
Deze interconnectiviteit overschrijdt landsgrenzen. Communicatiekabels en satellieten zijn niet gebonden aan landsgrenzen, en de data wordt ongeacht de oorsprong verzonden. Landen zijn ook vergaand wederzijds afhankelijk geworden van elkaars grensoverschrijdende vitale infrastructuren zoals telecom, energievoorziening, transportsystemen en data-uitwisselingen.

Nieuwe dreigingen voor governance

De opkomende trend in connectiviteit en wederzijdse afhankelijkheid heeft de deur geopend voor nieuwe governance bedreigingen die tien jaar geleden nog niet bestonden, zoals cybercrime, cyberterrorisme, cyberspionage en cyberoorlogsvoering. Hoewel deze dreigingen al bestaan in de analoge wereld, zorgt de digitale dimensie ervoor dat deze dreigingen losstaan van tijd en ruimte. Daarmee worden wij kwetsbaar voor potentiele aanvallers wereldwijd.

Een hyper-connected omgeving die niet langer alleen door de staat beheerd kan worden, roept de vraag op wie er dan wel verantwoordelijk is voor cyberspace? De multistakeholderbenadering, een samenwerking tussen nationale overheden, private partijen en maatschappelijke organisaties, kan een antwoord zijn op deze vraag. Deze benadering brengt alle actoren samen die essentieel zijn in het beveiligen van cyberspace en iedere partij heeft zijn eigen rol.

Schetsen en delen van verantwoordelijkheid

Overheden spelen een significante rol in het reguleren en stimuleren van onderzoek naar innovatieve technologieën. Lidstaten zijn in staat de internationale samenwerking met andere landen op het gebied van informatie-uitwisseling en capaciteitsopbouw te faciliteren en te vergemakkelijken.
De private sector produceert en ontwikkelt vrijwel alle technologieën. Dat geeft deze sector

By 2020, estimates show that the number of connected devices will rise to 25 billion, and the amount of data produced will reach 35 Zettabytes. These numbers indicate that more analogue devices will become digital and begin to communicate using cyberspace, adding to the current levels of interconnectivity.
This interconnectivity transcends Nation States. Communication cables and satellites are not limited to national borders, and the data is transmitted regardless of its origins. Nations have also become highly interdependent on foreign Critical Infrastructures such as Telecoms, Energy grids, Transport systems, and Data exchanges that operate across multiple borders.

New Threats to Governance

This rising trend in connectivity and interdependence has opened the door to new governance threats that were not present less than a decade ago, such as Cybercrime, Cyber-terrorism, Cyber-espionage and Cyber-warfare. Though these threats already exist in an analogue world, the digital dimension unbinds these threats from a particular time and space, making us vulnerable to potential attackers in countries across the globe.
A hyper-connected environment that can no longer be governed by the state alone leads us to the question of – who is responsible for governing Cyberspace? The Multistakeholder approach, cooperation between National Governments, Private Sector companies, and Civil Society Organizations, may be the answer to our question. This approach brings together all actors essential to securing cyberspace as they all have distinct roles to play.

Outlining and Sharing Responsibility

Governments play a significant role in regulating and stimulating research of innovative technologies. As the Nation States are the unit of measurement at the international level, they play

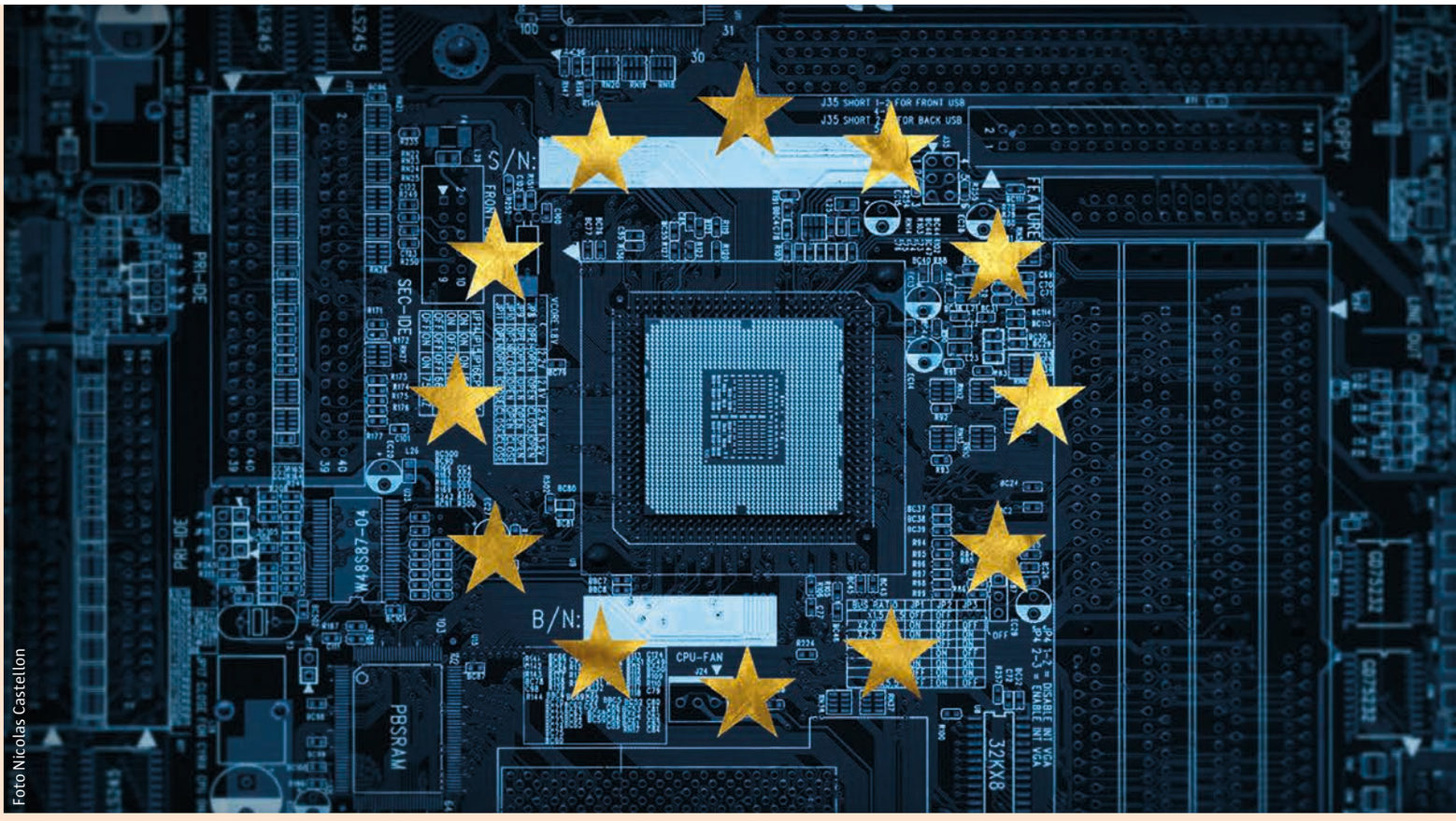


Foto Nicolas Castellon

een centrale rol in het produceren van veilige hard- en software en deze te beschermen tegen malware en andere vormen van cyberaanvallen. De private sector loopt voorop op het gebied van technische kennis. Dat maakt het bedrijfsleven een belangrijke speler in het verdiepen van ons begrip over cybersecurity en het ontwikkelen van veilige technologieën voor het verzenden van, toegang hebben tot en opslaan van data in cyberspace.
Maatschappelijke organisaties spelen een rol in het beschermen van de mensenrechten in cyberspace. Deze sector speelt een belangrijke rol in het pleiten voor het recht op privacy, vrijheid van meningsuiting en vrijheid van vereniging. Hoewel dit misschien geen directe rol speelt in het beveiligen van cyberspace, voegt dit wel een belangrijke dimensie toe aan het veiligheidsdebat.

Een nieuwe uitdaging voor governance

Cyberspace is de volgende uitdaging voor governance. Het vraagt om gelijkwaardige deelname van overheden, private partijen en maatschappelijke organisaties. Met deze multistakeholderbenadering worden governance-vraagstukken geadresseerd op maatschappelijk, technologisch en persoonlijk niveau. De verschillende stakeholders hebben ieder een belangrijke rol in het beveiligen van cyberspace en zouden gezamenlijk verantwoordelijkheid moeten dragen met betrekking tot het beheren van dit domein. De relatie tussen deze sectoren vormt een equilibrium dat zorgt voor een systeem van checks-and-balances dat noodzakelijk is om te navigeren in het relatief onbekende terrein dat cyberspace heet.

WIE IS ER VERANTWOORDELIJK VOOR CYBERSPACE?

WHO IS RESPONSIBLE FOR GOVERNING CYBERSPACE?

a role in facilitating international cooperation for information sharing and capacity building of other nations.
The Private Sector manufactures and develops virtually all technologies, giving this sector a central role in producing secure hardware and software, and protecting them against malware and other forms of cyber-attacks. The private sector takes the lead in terms of technical knowledge, making it a key player in deepening our understanding and developing secure technologies to transmit, access, and store data in cyberspace.

Civil Society Organizations play a role in the protection of Human Rights in cyberspace. This sector plays a key role in advocating rights to Privacy, Freedom of Speech and Freedom of Association. Though this may not play directly into securing cyberspace, their advocacy adds an important dimension to the security debate.

A New Frontier for Governance

Cyberspace is the next frontier for governance, and it demands equal participation from Nation States, the Private Sector, and Civil Society Organizations. With the Multistakeholder approach, governance issues are addressed at a societal, technological, and personal level. These different sectors have important roles to play in securing cyberspace and should share responsibility for governing this domain. The relationship between these sectors form an equilibrium that provides a system of checks and balances that this is necessary to navigate the unchartered waters of cyberspace.

Shutterstock

By **Paul Timmers**, director DG Connect, EU

De Europese Unie (EU) constateert dat online barrières een belemmering vormen voor één Europese digitale markt. “Burgers, bedrijfsleven en overheden kunnen daardoor niet volop gebruikmaken van alle digitale mogelijkheden die er zijn en dat schaadt de economie”, zegt Paul Timmers, directeur DG Connect. “Het is tijd daar verandering in aan te brengen.”

The European Union (EU) concludes that online barriers constitute a restriction for one European digital market. “As a result citizens, the business sector and authorities cannot fully make use of all digital options that exist and this hurts the economy”, according to Paul Timmers, managing director of DG Connect. “It is time to change this.”

SMART CITIES PART OF EU INITIATIVE ‘DIGITAL SINGLE MARKET’

REINFORCING INDUSTRIAL BASIS OF CYBER SECURITY

De EU is daarom het initiatief ‘Digital Single Market’ gestart met als doel de regelgeving te verminderen en van 28 naar één digitale markt te komen. Volgens berekeningen kan de Europese economie hierdoor per jaar met 415 miljard euro groeien en kan het honderdduizenden nieuwe banen opleveren. Om dit te realiseren is er een ‘digitale agenda’ opgesteld. Die bestaat uit drie pilaren: een consumenten- en bedrijvenpilaar die onder andere gaat over contracten en copyright in het kader van digitale handel en consumptie, een infrastructuurpilaar die onder andere gaat over het regelgevend kader voor telecommunicatie, internetplatforms, veiligheid en privacy en tot slot een economie- en maatschappijpilaar die onder andere gaat over data, standaarden en e-governement. De agenda bevat 16 concrete acties, waardoor de focus sterk ligt op het behalen van resultaat.

Slimme steden

Binnen de digitale agenda besteedt de EU uitgebreid aandacht aan het thema ‘smart cities’. Deze steden hebben een groot economisch en maatschappelijk potentieel, vanwege de slimme ontsluiting van data en diensten. Een uitstekende oplossingsrichting voor het leefbaarder en economisch succesvol maken van onze steden. Binnen dit thema komen diverse punten uit de agenda samen, vaak sector-overstijgend. Data,

The EU therefore started the initiative ‘Digital Single Market’, with the aim to reduce the barriers and combine 28 digital markets into one digital market. According to calculations, the European economy can grow as a result of this by 415 billion euros and create hundred of thousands of new jobs. One ‘digital agenda’ has been drawn up in order to realise this. It consists of three pillars: a consumer and company pillar which, amongst others, deals with contracts and copyright as part of digital trade and consumption, an infrastructure pillar which amongst others, deals with the regulatory framework for telecommunication, internet platforms, security and privacy and, finally, an economy and society pillar which, amongst others, deals with data, standards and e-government. The agenda includes 16 concrete actions, so that the focus is strongly on achieving a result.

Smart cities

Within the digital agenda the EU extensively highlights the theme of ‘smart cities’. These cities have a great economic and social potential, because of the smart access to data and services. This is an excellent problem-solving approach for making our cities liveable and economically successful. Within this theme the various points from the agenda come together, and often transcend the sectors. Data, standards, security, privacy, entrepreneurship and sharing economy can all be found in, for example, energy, transport, health and safety. For example, a number of cities and companies agreed with each other to make 10 million street lanterns “smart”


DG Connect

standaarden, security, privacy, ondernemerschap en sharing economy komen bijvoorbeeld terug in energie, transport, gezondheid en veiligheid. Zo hebben een aantal steden en bedrijven met elkaar afgesproken 10 miljoen straatlantaarns slim te maken met LED's, wifi, sensors en laadpunten voor elektrische auto's. Er ontstaat een hele nieuwe stadsstructuur. Vanuit Europa stimuleren we de ontwikkeling van deze creatieve en vernieuwende diensten.

Privaat-publieke samenwerking

Uiteraard speelt cybersecurity een belangrijke rol in de Europese digitale economie. De cybersecurity markt is echt versnipperd en verre van gestructureerd. In andere segmenten van de ICT-industrie is dat wel het geval. Zo zijn er op het gebied van micro-elektronica gevestigde regionale clusters en 'ecosystemen' te vinden van academische, industriële en institutionele partijen en gebruikers. Dat maakt het mogelijk concurrerend te zijn op de wereldmarkt. Voor

---

with LED's, wifi, sensors and introduce charging points for electric cars. This creates an entirely new city structure. We stimulate the development of these creative and innovative services.

Private-public cooperation

Cyber security obviously plays an important role in the European digital economy. However, the cyber security market is fragmented and far from structured. In other segments of the IT industry this is not the case. For example, established regional clusters and 'ecosystems' of academic, industrial and institutional parties and users can be found in the field of micro-electronics. This makes it possible to be competitive on the world market. We must also try to achieve something like this for the field of cyber security. An active interaction is therefore promoted in the Horizon 2020 programme between research, development, digital regulations and other policy instruments. Part of this is a reinforcement of the industrial basis in cyber security. In this context the European Committee has introduced a proposal for a 'contractual private-public partnership'. Industrial and public resources are brought together to jointly develop a 'roadmap', strategic research, innovation and education. This should stimulate the competitive and innovative power of the European digital security and privacy industry and create innovation products and services. Through this citizens and companies must gain access to up-to-date safe technology and infrastructure, based on the values which we in Europe consider to be important, such a protection of personal details and democracy.

CYBERSECURITY SPEELT EEN BELANGRIJKE ROL IN DE EUROPESE DIGITALE ECONOMIE

CYBER SECURITY PLAYS AN IMPORTANT ROLE IN THE DIGITAL SINGLE MARKET OF THE EU

cybersecurity moeten we ook zoiets zien te bereiken. Binnen het Horizon2020-programma wordt daarom een actieve wisselwerking tussen onderzoek, ontwikkeling, digitale regelgeving en andere beleidsinstrumenten gepromoot. Onderdeel daarvan is een versterking van de industriële basis in cybersecurity. De Europese Commissie komt in dat kader met een voorstel voor een 'contractual private-public partnership'. Industriële en publieke middelen worden bij elkaar gebracht om gezamenlijk te komen tot een 'roadmap', strategisch onderzoek, innovatie en onderwijs te komen. Dit moet de concurrentie- en innovatiekracht van de Europese digital security- en privacy-industrie stimuleren en zorgen voor innovatie producten en diensten. Burgers en bedrijven moeten daarmee toegang krijgen tot up-to-date veilige technologie en infrastructuur, gebaseerd op de waarden die we in Europa belangrijk vinden, zoals bescherming van persoonsgegevens en democratie.

Nieuwe ontwikkelingen

Naast de 'Digital Single Market' speelt er binnen Europa meer op het gebied van cybersecurity. Een van de belangrijkste ontwikkelingen is de EU-richtlijn voor netwerk- en informatiebeveiliging. Deze richtlijn heeft drie 'luiken': lidstaten moeten kunnen omgaan met impactvolle cyberincidenten, lidstaten werken met elkaar samen en als derde moeten vitale sectoren, waaronder transport, elektriciteit en een aantal internetsectoren, gaan voldoen aan regelgeving omtrent risicomanagement en notificatieplicht. Veel aandacht gaat uit naar privacywetgeving, waarvan de herziening de afgelopen paar jaar onderhandeld is. Een herziening van de e-privacy-richtlijn komt er nog aan. Hierbij wordt rekening gehouden met recente uitspraken van het Europese Hof over persoonlijke gegevensbescherming, onder andere in het kader van de ongeldig verklaarde Safe Harbour-afspraken tussen Europa en de Verenigde Staten.

Verder staat komende jaar de modernisering van de telecommunicatiewetgeving op de rol, als onderdeel van het 'Digital Single Market'-initiatief. Onderdelen van deze wetgeving hebben betrekking op cybersecurity.
Tot slot zien we het 'Internet der Dingen' opkomen. Organisaties en bedrijven zullen hun businessmodellen zien veranderen of op z'n minst profiteren van deze nieuwe technologische mogelijkheid. De realiteit van toenemende cyberdreigingen moeten zij daarbij onder ogen zien, liever vandaag dan morgen. Een gezamenlijk engagement, zoals binnen de Nederlandse Cyber Security Raad, is daarom ook binnen Europa meer dan welkom. Het is noodzaak!

New developments

Besides the 'Digital Single Market', there are other developments in Europe in the field of cyber security. One of the most important developments is the EU directive for network and informative security. This directive has three 'shutters': member states must be able to deal with cyber incidents that have a great impact, member states must work together with each other and, thirdly, vital sectors, including transport, electricity and a number of internet sectors, must comply with regulations regarding risk management and an obligation to notify.
Much attention is focused on privacy legislation, about which the review was the subject of negotiations in the past year. A review of the e-privacy directive will also be published soon. Action will also be taken following recent statements by the European Court regarding personal data protection, amongst others as part of the Safe Harbour arrangements between Europe and the United States, which have been declared to be invalid.
Furthermore, the modernisation of the telecommunication legislation will be planned next year, as part of the 'Digital Single Market' initiative. Parts of this legislation refers to cyber security.
Finally, there is the emergence of the 'Internet of Things'. Organisations and companies will see their business models change or at least profit from this new technological opportunity. They will have to face the reality of increasing cyber threats, and do this preferably today than tomorrow. A joint commitment, as in the Dutch Cyber Security Council, is therefore very welcome in Europe. It is absolutely vital!

SEBASTIAN REYN

new member of the Cyber Security Council

Sebastian Reyn is directeur Strategie, Beleidsontwikkeling en Innovatie van het ministerie van Defensie. Namens Defensie is Reyn in 2015 toegetreden tot de Cyber Security Raad. Hij volgt schout-bij-nacht Rob Bauer op, die plaatsvervangend Commandant der Strijdkrachten is geworden. *Sebastian Reyn is Director of Strategy, Policy Development and Innovation of the Ministry of Defence. Reyn joined the Cyber Security Council in 2015 on behalf of the Ministry of Defence. He succeeded Rear Admiral at night Rob Bauer, who became deputy Chief of the Netherlands Defence Staff (CDS).*

‘DIGITAL INSECURITY AFFECTS OUR PROSPERITY’

Waarom is ‘cyber’ een belangrijk thema voor Defensie?

“Onze digitale samenleving wordt steeds digitaler en er ontstaat een steeds groter wordende afhankelijkheid van ICT-systemen en technologie. Dat dringt ook door tot de krijgsmacht van Nederland en van andere landen. Cyber is inmiddels een onlosmakelijk onderdeel van het militaire optreden. Cyber is dus belangrijk voor Defensie. Maar Defensie is ook belangrijk voor cyber, want wij zijn in staat om met onze kennis en expertise een bijdrage te leveren aan de digitale veiligheid van Nederland. In het kader van nationale operaties kunnen overheden in geval van crises terugvallen op de krijgsmacht, dit geldt ook voor cybercrises.”

Wat is voor u het belang van de Cyber Security Raad?

“Defensie is niet de enige die een rol heeft in de nationale cybersecurity. Daarom is het mooi dat de Cyber Security Raad een brede samenstelling kent van publieke, private en wetenschappelijke partijen. Een gebrek aan digitale veiligheid raakt onze economie en onze welvaart, en daardoor raakt het iedereen. Juist daarom is de raad nodig, om op strategisch en bestuurlijk niveau de nationale strategie diepgaand te bespreken en te ontwikkelen op basis van wat er op ons land afkomt. Ook binnen organisaties hoort cybersecurity op topniveau belegd te zijn, als primair proces dat alles te maken heeft met de kern van wat je doet.”

Why is ‘cyber’ an important topics for Defence?

“Our society is becoming increasingly digitalised and there is an increasing dependence on ICT systems and technology. The armed forces of the Netherlands and other countries are also starting to realise this. In the meanwhile, cyber has become an inextricable part of military actions. Cyber is therefore also important for Defence. However, Defence is also important for cyber, because we are able to make a contribution to the digital security of the Netherlands through our knowledge and expertise. As part of national operations , the authorities can fall back on the armed forces in case of crises. This also applies to cyber crises.

Why is the Cyber Security Council important to you?

Defence is not the only party that plays a role in national cyber security. This is why it is a good thing that the Cyber Security Council has a broad composition of public, private and scientific parties. A lack of digital security affects our economy and prosperity, so it therefore affects everybody. It is in particular for this reason that the council is necessary: to discuss the national strategy on a strategic and administrative level in a thorough way and develop it on the basis of external events that affect our country. Cyber security should also be discussed on a top level within organisations, as a primary process that is related to all their key activities.

With **Freddy Dezeure**,
Head of CERT-EU

CERT-EU is het Computer Emergency Response Team van alle EU-instellingen. Freddy Dezeure, hoofd van CERT-EU, legt uit hoe het team helpt om zijn opdrachtgevers te beschermen tegen de steeds geavanceerdere cyberaanvallen. *CERT-EU is the Computer Emergency Response Team of the EU Institutions, Bodies and Agencies. Freddy Dezeure, Head of CERT-EU, explains how it helps to protect its constituents against ever more sophisticated cyber-attacks.*

PROTECTING THE EU INSTITUTIONS AGAINST CYBER THREATS

CERT-EU is in juni 2011 op initiatief van Neelie Kroes opgericht als onderdeel van de Europese digitale agenda. Het doel was om de cybersecurity van de EU-instellingen te vergroten. Ook gaf het een goed voorbeeld aan de lidstaten, met name aan lidstaten die geen nationaal of overheids-CERT hadden.
Het Europese Computer Emergency Response Team ondersteunt ongeveer zestig EU-instellingen, waaronder de Europese Commissie, het Europees Parlement, de ECB, Europol en ENISA. Het fungeert als hub voor informatie-uitwisseling inzake cybersecurity en coördineert de respons bij incidenten. CERT-EU is ondergebracht bij de Europese Commissie, maar wordt aangestuurd door een breed samengestelde stuurgroep van senior managers van de belangrijkste EU-instellingen.

Kunt u ons iets vertellen over de huidige dreigingen?
"De dreigingen waar CERT-EU mee te maken heeft zijn 'gerichte aanvallen', die meestal verband houden met cyberspionage. Het doel hiervan is het verkrijgen van toegang tot gevoelige informatie van geopolitieke, economische of technische aard. Deze aanvallen worden op zeer geavanceerde wijze uitgevoerd: detectie wordt vermeden en alles is er op gericht zo lang mogelijk in de systemen aanwezig te blijven. De EU-instellingen worden regelmatig aangevallen, maar gelukkig slagen de meeste aanvallen niet. Er bestaat echter geen absolute bescherming tegen geavanceerde gerichte aanvallen, gezien de dertig grote incidenten die we per jaar afhandelen."

Wat zijn de uitdagingen?
"Wat de uitdaging nog groter maakt, is dat de EU-instellingen steeds afhankelijker worden van ICT, waardoor ze kwetsbaarder worden en steeds vaker aangevallen worden. Ook zijn de tegenstanders steeds meer vastberaden om te slagen in hun opzet. We merken ook dat cyberaanvallen steeds vaker commercieel worden ingezet. Tegenstanders gebruiken geautomatiseerde tools om zwakke plekken in software, hardware

CERT-EU was launched in June 2011 as part of the European Digital Agenda, initiated by Neelie Kroes. The objective was to improve the cyber security of the EU institutions and to lead by example towards the Member States, in particular those that didn't have a national or governmental CERT.
It supports all EU institutions, bodies and agencies; around 60 organisations like for example the European Commission, the European Parliament, the ECB, Europol and ENISA. It acts as their cyber-security information exchange and incident response coordination hub. CERT-EU is hosted by the European Commission, but it functions as a common capacity under the guidance of a Steering Board, composed of senior managers of the main EU institutions.

Could you tell us something about the current threat landscape?
"The threats CERT-EU is dealing with are 'targeted attacks', in most cases related to cyber-espionage. They aim to gain access to sensitive information of geopolitical, economic or technical nature. These attacks are organised in a very sophisticated way, avoiding detection and maintaining presence in the infrastructure for as long as possible. Our constituents are frequently targeted; fortunately most attacks are unsuccessful. However, there is no absolute protection against sophisticated targeted attacks and we currently handle some 30 major incidents per year."

What are the challenges?
"What makes it all the more challenging is that our

en systemen op te sporen. Ze ontwikkelen zo snel aanvallen, dat het erg moeilijk is om ze bij te houden. Het is zeer moeilijk om cyberaanvallen op betrouwbare wijze te vinden. De ervaring van de afgelopen vier jaar heeft echter geleerd dat een groot aantal aanvallen waarschijnlijk uit China of Rusland komt. Maar waar de dreiging ook vandaan komt, wij volgen ze actief.
De laatste tijd hebben we een grote toename van het aantal cyberaanvallen geconstateerd, die vermoedelijk verband houdt met de politieke spanningen in Oost-Europa. Conflicten in de echte wereld worden ook in cyberspace uitgevochten. Hoewel we nog geen direct bewijs gezien hebben, verwachten we in de toekomst cyberaanvallen in relatie tot de spanningen in het Midden-Oosten.
Tot slot ben ik van mening dat we voorbereid moeten zijn op verstorende cyberdreigingen die de vitale infrastructuur treffen."

Hoe is het om voor CERT-EU te werken?
"Het grootste deel van het personeel bestaat uit IT'ers die gespecialiseerd zijn in het reageren op incidenten, het opsporen van indringers, het uitvoeren forensische analyse, het beoordelen

---

constituents are increasingly dependent on ICT, intrinsically vulnerable, and more and more targeted by determined adversaries. We are also experiencing an industrialisation of the exploit cycle. Adversaries are using automated tools to detect vulnerabilities in software and hardware and identify exposed systems. They develop exploits at such a pace that it is very hard to keep track.
Reliable attribution of cyber-attacks is very difficult. However, from the experience in the past four years, an important number of attacks are suspected to be of Chinese and Russian origin. But we actively monitor all significant and relevant threats.
We have recently seen an important uptick in cyber-attacks, which we believe are correlated with the political tensions in Eastern Europe. Conflicts in the real world are also fought in cyber-space.
Even though we have not seen direct evidence yet, we expect future cyber-attacks related to the tensions in the Middle East. I believe we should also be prepared for disruptive cyber threats, impacting critical infrastructure."

What is it like to work for CERT-EU?
"Most of our staff are IT engineers, specialised in incident response, intrusion detection, forensic analysis, vulnerability assessment, and cyber threat intelligence. We currently employ 20 staff, with additional recruitments in the pipeline. Working at CERT-EU is very exciting, continuously being challenged by sophisticated adversaries. It's also fun because we have a really cool team."

How do you enhance the security of the Institutions?
"CERT-EU helps them to prevent cyber threats, to detect them

CERT-EU HELPT DE EU-INSTELLINGEN OM CYBERDREIGINGEN TE VOORKOMEN, EERDER OP TE SPOREN EN SNELLER OP TE LOSSEN

CERT-EU HELPS THE EU INSTITUTIONS TO PREVENT CYBER THREATS, TO DETECT THEM AND TO RESOLVE THEM

van kwetsbaarheden en het informatie verzamelen over cyberdreigingen. Op dit moment hebben we twintig personeelsleden en er zal nieuw personeel geworven gaan worden. Het is erg enerverend om bij CERT-EU te werken, omdat je voortdurend uitgedaagd wordt door tegenstanders die geavanceerd technologieën gebruiken. Bovendien is het erg leuk, omdat we een ontzettend cool team hebben."

Hoe verbeter je de beveiliging van de instellingen?
"CERT-EU helpt de EU-instellingen om cyberdreigingen te voorkomen, eerder op te sporen en sneller op te lossen, waarbij we nauw samenwerken met hun eigen interne IT-teams. Wij bieden meerwaarde, vanwege ons zeer bekwame personeel, de gespecialiseerde tools die we inzetten, het sterke netwerk van collega's en partners, en de toegang tot unieke informatiebronnen. Ook helpen we ze bij het inzetten van gespecialiseerde veiligheidstools en -diensten.
We proberen getroffen systemen snel te identificeren met gebruik van slimme opsporingsregels en het monitoren van netwerken en hosts. Bovendien is het een belangrijk doel om kritieke incidenten snel aan te pakken.
We beperken ons echter niet tot technische ondersteuning. We gebruiken onze kennis en inzichten om tactische en strategische dreigingsbriefings op te stellen voor de hoogste bestuurlijke en politieke niveaus binnen de EU.

Hoe belangrijk is het om samen te werken met collega's en partners?
"Dat is zeer belangrijk. De meeste collega's worden aan dezelfde aanvallen blootgesteld als wij en hoe meer we elkaar op de hoogte houden, hoe beter we beschermd worden.
CERT-EU staat altijd in contact met collega's, nationale en overheids-CERT's van EU-lidstaten, NATO-NCIRC en US-CERT. Dagelijks vindt er informatie-uitwisselingen plaats.
CERT-EU onderhoudt eveneens uitgebreide contacten met gespecialiseerde IT-beveiligingsbedrijven, zoekt contact met de beste deskundigen ter wereld, krijgt toegang tot dreigingsinformatie en risicobeperkende maatregelen. Deze samenwerking wordt geregeld door wederzijdse geheimhoudingsovereenkomsten, die in het algemeen niet-commercieel zijn omdat de samenwerking een wederzijds belang heeft.
De mensen zijn het allerbelangrijkst bij deze samenwerking: een hecht netwerk van bekwame, betrouwbare en daadkrachtige deskundigen."

earlier and to resolve them quicker, interacting closely with their internal IT teams. It provides value through its highly skilled staff and specialised tools, its strong network of peers and partners and its access to unique sources of information. We also help them to deploy specialised security tools and services.
We try to identify compromised systems by using clever detection rules to monitor networks and hosts. Escalating critical incidents quickly and responding to them swiftly is also a key goal.
We don't limit ourselves to technical support, though. We convert our knowledge and insights into tactical and strategic threat briefings that find their way to the highest management and political levels in the EU.

How important is collaboration with peers and partners?
"It's very important. Most of our peers are exposed to the same attacks as we do and the more we keep each other informed the better we are protected.
CERT-EU is continuously in contact with its peers, the EU national/governmental CERTs, NATO-NCIRC and US-CERT. And you have to take this literally; exchanges are taking place on a daily basis.
CERT-EU also maintains extensive contacts with specialised IT security companies, reaching out to the best experts on the planet, obtaining privileged access to threat intelligence and mitigation measures. This cooperation is organised under mutual non-disclosure agreements, generally under non-commercial terms as the cooperation is of real mutual interest.
Most important in this cooperation are the people: a tight network of competent, trustworthy and highly actionable experts."

Mausbaus

By **Danny Ter Laak**, National Office of the Public Prosecution Service

Het Openbaar Ministerie staat voor een integrale aanpak van criminaliteit, vanuit de gedachte dat criminaliteit alleen effectief kan worden bestreden door samenwerking tussen publieke en private partijen. Het zogenaamde barrièremodel is een voorbeeld van zo'n integrale aanpak, waarbij diverse partners barrières opwerpen om criminelen te hinderen en te stoppen. Dit in de praktijk bewezen model is ook toepasbaar op de aanpak van cybercrime. *The Public Prosecution Service supports a comprehensive tackling of crime, on the basis of the idea that crime can only be tackled effectively through cooperation between public and private parties. The so-called barrier model is an example of such a comprehensive tackling, whereby various partners raise barriers to hinder and stop criminals. This model which has proved its value in practice can also be applied in cybercrime.*

BARRIER MODEL OFFERS OPPORTUNITIES AGAINST CYBERCRIME

Via het barrièremodel zijn partijen in staat het businessmodel van criminelen te analyseren en te splitsen in fasen. Binnen die fasen wordt het criminele proces op zoveel mogelijk momenten verstoord. Zo kan het barrièremodel ingrijpen op bijvoorbeeld het motief van een dader, beschikbaarheid van middelen of instrumenten, doelen en opbrengsten. Neem het voorbeeld van een DDoS-aanval, bijvoorbeeld uitgevoerd door een jeugdige. Wat is het motief van de dader? Hoe kan het dat de benodigde software voor deze aanvallen via illegale websites te verkrijgen is? Wordt er op het basis- en voortgezet onderwijs voldoende aandacht besteed aan de wettelijke en morele grenzen van digitaal handelen? Stellen bestuurders van grote bedrijven in de boardroom zichzelf wel eens de vraag hoe zij kunnen bijdragen aan het tegengaan van cybercrime? En welke barrières kunnen hostingpartijen en internetproviders treffen?

Het instrument

Het barrièremodel werpt gerichte hindernissen op om specifieke criminele activiteiten tegen te gaan. Een belangrijk fundament is het in kaart brengen van legale en illegale criminele structuren en partijen die dit faciliteren. Met legale of onbewuste facilitators zoekt het Openbaar Ministerie actief de samenwerking. Daarentegen worden illegale of bewuste facilitators van criminaliteit aangesproken of aangepakt. Het Openbaar Ministerie (OM) heeft inmiddels verschillende succesvolle voorbeelden van deze integrale aanpak van criminaliteit.

With the barrier model parties can analyse the business model of criminals and divide it according to phases. The criminal process is disrupted as frequently as possible in these phases. For example, the barrier model can interfere with the motive of an offender, availability of resources or instruments, objectives and profits. Take a Distributed Denial of Service (DDoS) attack, for example, which is carried out by a young person. What is the motive of the offender? How is it possible that the required software for these attacks can be obtained through illegal websites? Do primary and secondary schools pay sufficient attention to the statutory and moral boundaries of digital actions? Do directors of large companies in the boardroom sometimes wonder how they can contribute to fighting cybercrime? And which barriers can hosting parties and Internet Service Providers put up?

Instrument

The barrier model creates specific barriers to counter specific criminal activities. An important basis is assessing legal and illegal criminal structures and parties that facilitate this. The Public Prosecution Service actively seeks cooperation with legal or unintentional facilitators. On the other hand illegal or intentional facilitators of crime are called to account or legal action is taken against them. In the meanwhile the Public Prosecution Service

EFFECTIEVE INTERVENTIES VRAGEN OM DURF EN SAMENWEWRKING

EFFECTIVE INTERVENTIONS REQUIRE GUTS AND COOPERATION

In de aanpak van mensenhandel werkt het OM onder andere samen met gemeenten en de Kamer van Koophandel. Samen met Horeca Nederland en andere partijen werkt het OM aan de aanpak en voorkoming van illegale hotelprostitutie. En binnen het internationale project Illegal Trade on Online Marketplaces werpen Douane, PostNL en OM barrières op om de aan- en verkoop van illegale producten op het dark web tegen te gaan en op te sporen. Ook kinderporno, skimming, drugshandel en identiteitsfraude worden middels barrièremodellen aangepakt.

Aanpak cybercrime

De ontwikkeling van een barrièremodel op het gebied van cybercrime staat nog in de kinderschoenen. Een dergelijk model biedt kansen, bijvoorbeeld bij het voorkomen van DDoS-aanvallen, de aanpak van de ontwikkeling en verkoop van malware of het gebruik van ransomware. Het OM zoekt actief naar samenwerking met partijen die hierin een rol kunnen spelen. Een barrièremodel kan namelijk niet door één partij achter de tekentafel worden ontworpen. De aanpak van een criminaliteitsvorm als cybercrime, met alle complexe uitdagingen waar we vandaag de dag internationaal voor staan, vraagt om een dialoog tussen alle partijen die in meer of mindere mate een bijdrage kunnen leveren aan het verstoren van deze criminele handelingen. Het vergt soms durf en lef om te komen tot effectieve interventies en samenwerking tussen partijen die in eerste instantie zelf misschien niet bewust waren van het feit dat zij een hele belangrijke bijdrage kunnen leveren aan het tegengaan en voorkomen van cybercrime. Ook vergt het internationale samenwerking; cybercrime stopt niet bij geografische grenzen. Als alle relevante partijen hun verantwoordelijkheid nemen, dan kunnen we ook voor cybercrime een (internationaal) barrièremodel tot stand brengen.

(OM) has several successful examples of this comprehensive tackling of crime. In tacking human trafficking the Public Prosecution Service works together, amongst others, with local authorities and the Chamber of Commerce. Together with Koninklijke Horeca Nederland (Dutch trade association for the hotel and catering industry) and other parties the Public Prosecution Service is working on tackling and preventing illegal hotel prostitution. Moreover, through the international project 'Illegal Trade on Online Marketplaces' the Tax and Customs Administration, PostNL and the OM are also creating barriers to counter and trace the purchase and sale of illegal products on the dark web. Child pornography, skimming, drugs trade and identity fraud are also being tackled through barrier models.

Tackling cybercrime

Developing a barrier model in the field of cybercrime is still in its infancy. Such a model offers opportunities, for example in preventing DDoS attacks, tackling the development and sale of malware or use of ransomware. The The Public Prosection Service is actively seeking cooperation with parties who may play a role in this. This is because a barrier model cannot be designed by one party behind the drawing table. Tackling a type of crime such as cybercrime, with all the complex challenges we are facing today internationally, requires a dialogue between all parties that can make a contribution to disrupting these criminal actions to a greater or lesser extent. It sometimes requires guts to realise effective interventions and cooperation between parties who initially were not aware of the fact that they could make a very important contribution to countering and preventing cybercrime. It also requires international cooperation; cybercrime does not stop at geographic borders. When all relevant parties assume their responsibility, we will be able to also establish an (international) barrier model for cybercrime.

LOKKE MOEREL

new member of the Cyber Security Council


Miranda Koopman

‘WE’RE LOOKING AT THE BIGGER PICTURE’

Lokke Moerel maakt deel uit van het global data privacy & security team van het advocatenkantoor Morrison & Foerster LLP, een Amerikaans technologiekantoor dat leidend is op het gebied van global cybercrime. Ook is zij hoogleraar ‘global ICT law’ aan Tilburg University. *Lokke Moerel is a member of the global data privacy & security team at the law firm Morrison & Foerster LLP, an American trend-setting technology office in the field of global cyber crime. She is also a professor of ‘global IT law’ at Tilburg University.*

Volgens de advocatenranglijsten Chambers Global en Legal 500 neemt u steevast een hoge positie in als het gaat om IT en databescherming. Waar komt uw fascinatie voor deze onderwerpen vandaan?

“Ik ben gefascineerd door nieuwe technieken en hun impact op de samenleving. Techniek is niet goed of slecht. Het gaat erom hoe je het toepast. In dat kader schrijf ik samen met collega-hoogleraar Corien Prins een preadvies voor de Nederlandse Juristen Vereniging over de nieuwe data gedreven samenleving. Invalshoek is big data, Internet of Things en hoe privacy-regulering daarop volgens ons moet worden aangepast. De huidige regelgeving is niet langer houdbaar, omdat het te weinig bescherming biedt aan burgers.”

Wat is voor u het belang van de Cyber Security Raad?

“De raad kijkt vooruit en denkt strategisch na over cybersecurity vanuit het overkoepelende perspectief van de BV Nederland. Ieder lid zet zijn eigen pet af en brengt zijn eigen ervaring en expertise in voor het grotere geheel. Ik merk dat dit echt een toegevoegde waarde heeft. Nederland loopt hiermee voorop en ik ken landen die jaloers kijken naar hoe wij dit geregeld hebben. Voor mij is het leuk dat ik mijn wereldwijde ervaring met cybercrimeaanvallen op data-gedreven bedrijven (en hoe bijvoorbeeld de FBI hierbij opereert) kan inbrengen.”

According to lawyer rankings “Chambers Global” and “Legal 500”, you invariably hold a senior ranking where it concerns IT and data protection. Where does your fascination for these subjects come from?

“I am fascinated by new techniques and their impact on society. Technology is neither good nor bad. What matters is how you apply it. In that respect, I’m drawing up a preliminary advice with fellow professor Corien Prins for the Dutch Lawyers Association about the new data-driven society. The angle of approach is Big Data, the Internet of Things and how we think associated privacy regulations should be adapted to it. Current regulations are no longer tenable, because it does not provide sufficient protection to citizens.”

What is the importance of the Cyber Security Council to you?

“The council looks ahead and thinks strategically about cyber security from an overseeing perspective of the Dutch business community. Every member unselfishly contributes its own experience and expertise for the greater good. I’ve noticed that this genuinely gives added value. With this, the Netherlands is a front-runner and I know some countries are jealously looking at how we’ve organised this. For me it’s great that I can contribute my worldwide experiences with cyber crime attacks on data-driven companies (and how, for example, the FBI operates in this).”

FBI Supervisory Special Agent J. Keith Mularski, hoofd van het cyber criminaliteit team op het kantoor in Pittsburgh, toont een screenshot van de Darkcode website, een Engelstalige markt voor cybercriminelen. Volgens autoriteiten van de Nationale Cyber Forensics & Training Alliance in Pittsburgh is Darkcode het grootste bekende Engels sprekende malware forum in de wereld. Het Amerikaanse ministerie van Justitie volgt in 20 landen meer dan 70 vermeende cybercriminelen die gebruik hebben gemaakt van het forum. Darkcode is een members only online marktplaats van gehackte databases, kwaadaardige software en andere middelen die computersystemen kunnen verlammen of informatie kunnen stelen.

FBI Supervisory Special Agent J. Keith Mularski, who heads the cybercrime squad at the agency s Pittsburgh field office, displays a screenshot from the Darkcode website, an English language marketplace for cybercriminals , the largest known "English speaking malware forum in the world, authorities said, at the National Cyber Forensics & Training Alliance in Pittsburgh, Tuesday, July 14, 2015. The Justice Department has targeted more than 70 alleged cybercrimals in 20 countries who ve been using Darkcode, a members only online marketplace to buy and sell hacked databases, malicious software and other products that can cripple or steal information from computer systems.

Hollandse Hoogte

By **Lokke Moerel**, Senior of counsel at Morrison & Foerster LLP, Berlin

Per 1 januari 2016 wordt in Nederland een wettelijke meldplicht voor datalekken van kracht. De boete op het niet naleven kan oplopen tot 10 procent van de wereldwijde bedrijfsomzet. Nederland loopt daarmee vooruit op de aankomende Europese Verordening Gegevensbescherming die een vergelijkbare meldplicht heeft. In Amerika bestaat al veel langer zo'n meldplicht, met grote gevolgen. Prof. dr. Lokke Moerel van het Amerikaanse advocatenkantoor Morrison Foerster ziet een aantal ontwikkelingen die ook van betekenis kunnen zijn voor Europa. *A legal obligation to notify data security breaches comes into effect in the Netherlands on 1 January 2016. The penalty for failure to comply may be up to 10 per cent of worldwide turnover. The Netherlands is therefore leading the way on the upcoming European Regulation on Data Protection, which includes a comparable notification obligation. Data breach notification requirements exist already for a long time in the United States and with great results. Prof. Lokke Moerel of the US based technology law firm Morrison Foerster sees a number of developments that can also be important for Europe.*

IMPORTANT AMERICAN DEVELOPMENTS FOR EUROPE

Wat Moerel als eerste opvalt in Amerika, zijn de recente stepping stone-hacks. Hackers bemachtigen informatie die hen in staat stelt geloofwaardige phishing e-mails te sturen naar werknemers van de organisatie waar ze willen binnendringen. "Toen in Amerika verzekeraar Anthem werd gehackt, vroegen we ons af wat de hackers hiermee wilden bereiken. Uiteindelijk bleek dat zij met de gestolen informatie zeer gerichte phishing e-mails konden versturen aan Amerikaanse ambtenaren. Dit leidde tot de grootste infiltratie van de Amerikaanse overheid ooit, waarbij ook de personeelsdossiers van 21,5 miljoen Amerikaanse ambtenaren werden gestolen." Deze stepping stone-hack laat zien dat iedere organisatie – bedrijfsleven én overheid – interessant is om gehackt te worden. Lang niet iedereen is zich daarvan bewust, ziet Moerel in haar advocatenpraktijk. "Ze denken: ik ben niet interessant voor hackers... wel dus."

What Moerel first notices in the United States are the recent stepping stone-hacks. Hackers possess information enabling them to send credible phishing e-mails to employees of the organization that they wish to penetrate. "When the insurer Anthem in the United States was hacked, we wondered what the hackers wanted to achieve with this. It finally emerged that they were able to use stolen information to send very specific phishing e-mails to US officials. This led to the greatest ever infiltration of the US Government whereby the personnel files of 21.5 million US officials were stolen." This stepping stone-hack shows that there is an interest in hacking every organization – businesses and governments. Moerel sees in her practice that there is not sufficient awareness on this. "They think: we are of no interest to hackers... well they are."

Enormous consequences

There are no general legal provisions in the United States requiring organizations to adequately secure their data properly. Only when businesses lose specific combinations of personal identifiable information, for example due to hacking, are they required to report this to the individuals concerned. Such notifications in practice immediately trigger several class actions where citizens make claims for damage suffered. This so-called harm-based approach to regulation works better than the rights-based rules in Europe, says Moerel. "In Europe, we have a general security obligation

Miranda Koopman

Enorme consequenties

In Amerika is er geen algemene wettelijke bepaling die zegt dat organisaties hun data goed moeten beveiligen. Pas als bedrijven bepaalde persoonsgegevens kwijt zijn, bijvoorbeeld door een hack, moeten zij dit melden aan de personen waar het om gaat. Dit leidt in de praktijk direct tot grote aantallen class-actions waar burgers hun schade claimen. Deze zogenoemde harm-based benadering werkt beter dan de rights based regelgeving in Europa, zegt Moerel. “Wij kennen in Europa een algemene beveiligingsplicht van persoonsgegevens. Burgers hebben recht op goed beveiligde gegevens. Dat lijkt sterker dan in Amerika, maar in de praktijk is dat niet het geval. Deze algemene verplichting wordt namelijk onvoldoende nageleefd. De Amerikaanse naming and shaming als het misgaat, blijkt effectiever. Om te voorkomen dat ze een datalek publiek moeten maken, hebben Amerikaanse bedrijven veel in hun beveiliging geïnvesteerd. Die ligt daardoor vaak op een hoger niveau dan in Europa.” De nieuwe Europese verordening heeft beide elementen in zich en is dan ook een sterke stimulans voor organisaties om hun zaken goed op orde te hebben. Wel waarschuwt Moerel dat Europa niet moet doorschieten, zoals in Amerika dreigt te gebeuren. “Daar is soms sprake van een ‘over-notificatie’. Dit wordt veroorzaakt door een

with respect to personal data. Citizens have a right to have their data properly secured. This appears stricter than in the United States but this is not the case in practice. This general obligation is not adequately complied with in practice. The US system of naming and shaming when a data breach occurs is more effective. US companies have invested heavily in their security in order to avoid having to go public with a data leak. The security of US companies is often on a better level than in Europe.” The new European

NAMING AND SHAMING WERKT HET BESTE

NAMING AND SHAMING WORKS BEST

te laag vastgestelde drempel die aangeeft wanneer er moet worden gemeld. Wat mij betreft geldt de meldplicht als er een serieuze kans is op aanmerkelijke schade voor het individu. Het enkele verlies van een e-mailadres voldoet daar niet aan."

Bestuursverantwoordelijkheid

De Securities and Exchange Commission (SEC) is de Amerikaanse toezichthouder op de effectenbeurzen. Onder andere als gevolg van de Target-case, de Amerikaanse retailer waarbij persoonlijke gegevens van 70 miljoen klanten en 40 miljoen creditcardnummers werden gestolen, heeft de SEC verscherpte richtlijnen uitgevaardigd voor het bestuur van bedrijven. De SEC-richtlijnen verplichten bedrijven in al hun verplichte publicaties (zoals jaarverslag en periodieke meldingen) openheid van zaken te geven over hun cybersecurity-incidenten, ook die uit het verleden. Daarnaast heeft de US Standards and Technology (NIST) een Cybersecurity Framework ontwikkeld voor zestien vitale infrastructuursectoren, die een reflex werking lijken te hebben voor andere sectoren. Moerel verwacht dat dergelijke regelgeving en standaarden ook naar Europa zullen overwaaien. "De SEC stelt dat leden van de board op het gebied van cybersecurity een bestuurdersverantwoordelijkheid hebben. Zij kunnen zaken niet afschuiven op hun Chief Information Officer of Chief Security. De board zelf moet op de hoogte zijn van de cybersecurity-problematiek, risico's voor het bedrijf actief in kaart brengen en erop toezien dat deze goed worden gemanaged. Doet de board dat niet, dan vullen zij hun taak als bestuurders onvoldoende in. Verder mag de board niet alleen vertrouwen op interne tests, maar moeten ook externe penetratietests worden uitgevoerd." Volgens Moerel doen boards er goed aan een crisismanagement-simulatie te houden. Zonder deze ervaring is het onmogelijk om gecoördineerd een cybercrime-incident te managen. Verder verwacht Moerel, kijkend naar Amerika, dat de nieuwe meldplicht voor datalekken zal leiden tot meer transparantie over wat er digitaal gaande is. De cyberverzekeringsmarkt in Europa zal daardoor snel volwassen worden. "Amerika laat zien dat dit positieve effecten heeft op het beveiligingsniveau van bedrijven. Verzekeraars stellen namelijk eisen aan hun klanten. Overigens zijn de uitkeringen bij lange na niet voldoende om de financiële schade te dekken, laat staan de imagoschade. Dit zorgt er hopelijk voor dat de cybersecurity van organisaties wordt verbeterd, want dat is hard nodig."

regulation contains both elements and is therefore also a strong incentive for organizations to have their security in order. Moerel does however warn that Europe must not go too far in its notification obligations as is now in danger of happening in the United States. "There, you sometimes find 'over-notification'. This is due to certain States setting too low a threshold when something must be notified. As far as I am concerned, the obligation to report should only applyif there is a serious chance of considerable damage for the individual. The simple loss of an e-mail address should not be enough."

Management responsibility

The Securities and Exchange Commission (SEC) is the US stock exchange supervisory body. In the wake of the Target-case, whereby the personal details of 70 million clients and 40 million credit card numbers of this US retailer were stolen, the SEC has issued stricter directives for corporate management. The SEC directives oblige companies to provide transparency as to their cybersecurity incidents (including those in the past) in all their mandatory publications (such as annual reports and periodic notifications). Furthermore, the US Standards and Technology (NIST) has developed a cybersecurity framework for 16 vital infrastructure sectors, which already appears to have a reflex effect on other sectors. Moerel expects that such rules and standards will also find their way to Europe. "The SEC states that the Members of the Board of Directors have a management responsibility as far as cybersecurity is concerned. They cannot pass the buck onto their Chief Information Officer or Chief of Security. The Board of Directors itself must be aware of cybersecurity problems, actively map out the risks to the company and ensure that these are managed properly. The Board of Directors are neglecting their managerial responsibilities if they fail to do so. The Board of Directors may also not rely solely on internal tests; external penetration tests must also be carried out." Moerel believes that Boards of Directors would do well to hold a crisis management simulation. It is impossible to manage a cybercrime incident in a coordinated manner without this experience. Moerel also expects, looking at the United States that the new obligation to report regarding data leaks will provide more transparency as to what is going on in the digital world. The cyber-insurance market in Europe will therefore grow up quickly. "The United States shows that this has positive effects on security levels within companies. Insurers place requirements on their clients. The payments received are also no way enough to cover the financial loss, let alone the damaged image. It is hoped that this will improve cybersecurity within organizations as this is sorely needed."

Op dit moment is digitale verandering steeds meer verankerd in alle delen van ons leven door het dagelijks gebruik van tablets en smartphones of de aanhoudende overgang naar het internet der dingen. Toch ziet nog niet iedereen het belang van cybersecurity als een van de grootste uitdagingen van digitale verandering en als belangrijkste veiligheidskwestie in Europa. De EU-richtlijn inzake netwerk- en informatiebeveiliging (NIB) is cruciaal voor het opstellen van EU-brede minimumnormen voor veerkracht en om bij te dragen aan een functionerende, concurrerende Single Market. *Today, the digital change is more and more embedded in all parts of our life by the daily use of tablets and smartphones or the on-going transition towards the Internet of Things. Yet, not everyone has understood the importance of cyber security for users, companies or governments as one of the major challenges of the digital change and as key question for security in Europe. The EU Directive on Network and Information Security (NIS) is a crucial element in setting EU-wide minimum standards for resilience and to contribute to a functioning, competitive Single Market.*

CYBER SECURITY: NEW STANDARDS FOR A COMMON MARKET

Ondernemingen en overheden krijgen steeds vaker te maken met risico's die veroorzaakt worden door cyberaanvallen, of deze nu politiek of economisch gemotiveerd zijn. Voor Europese bedrijven - grote bedrijven of het midden- en kleinbedrijf - kunnen cyberaanvallen enorme economische gevolgen hebben. Ook zijn de IT-structuren van overheden en regeringen steeds vaker het doelwit van aanvallen door inlichtingendiensten. Aangezien cyberaanvallen niet stoppen bij nationale grenzen, zou het gevaarlijk zijn om niveauverschillen tussen de lidstaten te accepteren. Voorbereiding en veerkracht dienen overal zo groot mogelijk te zijn.

NIB-richtlijn

Met het oog hierop vormt de invoering van de NIB-richtlijn die de Europese Commissie in 2013 heeft voorgesteld een belangrijk element in de hele cybersecurity-strategie en -cultuur die we nu op ieder niveau moeten implementeren. De nieuwe richtlijn stelt een aantal verplichtingen vast, met name op het gebied van vitale infrastructuur, zoals energie, vervoer, bankwezen en gezondheid. Exploitanten in deze sectoren zijn verplicht om incidenten met een aanzienlijke impact te melden en dienen regelmatig beveiligingsaudits te ondergaan om de veerkracht van hun IT-systemen te garanderen. Digitale service-

More and more often, companies and governments are faced with growing risks caused by cyber-attacks - whether politically or economically motivated. For European businesses - large companies or SMEs - cyber-attacks can entail enormous economic consequences. Also the IT structures of governments and administrations are increasingly subject to attacks by intelligence services. As cyber-attacks do not stop at national borders and it would be dangerous to accept discrepancies between the Member States'. Preparedness and resilience should be as high as possible.

NIS Directive

In this light, the successful adoption of the NIS Directive - proposed by the EU Commission in 2013 - will constitute a major element in the whole cyber security strategy and culture that we need to implement now at all levels. The new Directive will set a number of obligations, mainly in the area of critical infrastructure such as energy, transport, banking or health. Operators in these fields will be subject to mandatory notifications of significant incidents and regular security audit to ensure resilience of their IT systems. Digital service providers, such as online marketplaces, will fall under a lighter regime but still need to take appropriate security measures. Member States as well as Computer Emergency Response Teams (CERTs) need to cooperate more closely to achieve a harmonised approach for resilience measures throughout

By **Dr. Andreas Schwab** MEP,
Rapporteur of the European
Parliament for the NIS Directive

WE MOETEN EEN INVESTERINGS-VRIENDELIJK KLIMAAT CREËREN

WE HAVE TO CREATE AN INVESTMENTFRIENDLY-ENVIRONMENT

providers, zoals online marktplaatsen, vallen onder een lichter regime maar dienen eveneens gepaste veiligheidsmaatregelen te treffen. Lidstaten en Computer Emergency Response Teams (CERT's) dienen nauwer samen te werken voor een geharmoniseerde aanpak van beveiligingsmaatregelen in de hele EU. Het Europees Parlement roept sterk op om meer samen te werken en te zorgen voor een echte Europese aanpak. Wel blijft tegelijkertijd de wens overeind om flexibiliteit van de lidstaten met betrekking tot nationale veiligheidskwesties te respecteren.

Grootste uitdaging

Cybersecurity is een van de grootste uitdagingen van dit moment die iedereen treft: politiek, bedrijfsleven en gebruikers. We zijn allemaal verantwoordelijk voor het creëren van een cultuur van cybersecurity en het zorgen voor vertrouwen: we moeten zorgen voor bewustwording in alle lagen van de maatschappij, overheid en industrie, bijvoorbeeld door middel van campagnes zoals de Europese maand van de cybersecurity. We moeten bestaande vormen van samenwerking verbeteren en nieuwe initiatieven opzetten, zoals publiek-private samenwerkingsverbanden. Autoriteiten en CERT's hebben - ook in het belang van de industrie - voldoende middelen nodig om hun taken efficiënt uit te voeren. We moeten op middellange en lange termijn synergieën versterken en een investeringsvriendelijk klimaat voor onderzoek en ontwikkeling creëren voor het opzetten van een gemeenschappelijk Europese cybersecurityindustrie. Ten slotte moeten we de NIB-richtlijn snel aannemen om het Europese kader voor gemeenschappelijke cyberveiligheidsnormen vast te stellen. Het Europees Parlement blijft als medewetgever alles in het werk stellen om bij lidstaten aan te dringen op dit ambitieuste, maar tegelijkertijd evenwichtige regelgevende kader.

the EU. This call for more cooperation has been strongly made by the European Parliament to ensure a true European approach, whilst respecting the Member States' wish for flexibility with regards to national security issues.

Main challenge

Therefore, cyber security is one today's main challenges and affecting everyone: politics, business, and users. We all have a common responsibility to create a true cyber security culture and hence establish trust: We need to raise the awareness at all levels of society, government and industry, for instance through campaigns such as the European cyber security month. We have to improve existing forms of cooperation and create new initiatives, such as public-private partnerships. Authorities and CERTs need sufficient resources to efficiently fulfil their tasks, also in the interest of industry. We have to strengthen synergies and create an investment-friendly environment for research and development in the mid-term and long-run in a view to create a common European cyber security industry. And finally, we need to swiftly adopt the NIS Directive to set the European frame for common cyber security standards. The European Parliament as the co-legislator will continue to do its utmost to push Member States for the most ambitious yet balanced regulatory framework.

Hollandse Hoogte

By **Wil van Gemert**,
Deputy Director of Operations at Europol

De krantenkoppen medio oktober 2015 in het Verenigd Koninkrijk (VK) zijn alarmerend: 'The UK is officially under cyber attack'. Aanleiding voor deze koppen is de publicatie van criminaliteitscijfers door het nationale bureau voor de statistiek. Voor het eerst wordt daarin een schatting gemaakt van de mate waarin burgers in het VK worden geconfronteerd met cybercriminaliteit. Het incorporeren van deze cijfers in de officiële criminaliteitsstatistieken levert na jaren van constante daling een enorme groei op van ruim 40%. Daarmee is cybercriminaliteit in één klap de meest voorkomende criminaliteitscategorie. *The UK headlines in mid October 2015 were alarming: 'The UK is officially under cyber attack'. The reason for the headlines is the publication of crime figures by the national bureau of statistics. For the first time an estimate has been made of the extent to which citizens in the UK are confronted by cybercrime. After years of steady decline, incorporating these figures into the official crime statistics reveals an enormous growth of more than 40%. Cybercrime has become the most prevalent category of crime at a single stroke.*

EUROPOL, CYBERCRIME AND STRATEGIC PARTNERSHIPS:

THINK BIG, ACT BIG

Het VK vormt waarschijnlijk geen uitzondering binnen Europa. De mate waarin inzicht bestaat in cybercriminaliteitscijfers varieert van land tot land. Toch is inzicht in de feitelijke verschijningsvorm en ernst van het probleem een voorwaarde voor een effectieve aanpak. Om aan die effectieve aanpak gestalte te geven is begin 2013 binnen Europol het Europese Cyber Crime Center (EC3) opgericht. Het mandaat van Europol heeft daarbij betrekking op georganiseerde criminaliteit, terrorisme of andere vormen van ernstige criminaliteit waarbij meer dan één EU-lidstaat is betrokken. Als ondersteunende dienst richt Europol zich op informatieverzameling, cross-matching, analyse, het leveren van expertise en directe operationele coördinatie en ondersteuning.

Drivers en trends

De terreinen waarop EC3 zich beweegt, zijn aanvallen en bedreiging van de infrastructuur door bijvoorbeeld DDoS-aanvallen en malware, grootschalige (card)fraude en seksueel misbruik van kinderen. Juist bij deze laatste vorm speelt cyber een enorme rol. Naast deze drie operationele prioriteiten wordt binnen EC3 aandacht besteed aan het vergaren van strategische informatie,

In all probability the UK is no exception inside Europe. Access to crime figures varies from country to country, but a clear understanding of the various forms of cybercrime and the seriousness of the problem is a necessary precondition for an effective approach. In early 2013 the European Cyber Crime Centre (EC3) was set up inside Europol to realise such an effective approach. The mandate of Europol thereby extends to organised crime, terrorism and other forms of serious crime in which more than one EU member state is involved. As a support service, Europol focuses on collecting information, cross-matching and analysis, as well as providing expertise and direct operational coordination and assistance.

Drivers and trends

The areas in which EC3 operates are: attacks and threats to infrastructure such as DDOS attacks and malware, large-scale (card) fraud and sexual abuse of children. In relation to the latter cyber activity plays an enormous role. Apart from these three operational priorities EC3 also focuses on collecting strategic information, cyber intelligence, strategic cooperation with private partners and forensic research. Our strategic flagship is the IOCTA, the 'Internet Organised Crime Threat Assessment'. The second edition thereof was published in the autumn of 2015 in partnership with Interpol. Developments, trends and threats are described

ER IS SPRAKE VAN EEN TRENDBREUK

THERE IS A COMPLETE DEPARTURE FROM THAT TREND

cyberintelligence, strategische samenwerking met private partners en forensisch onderzoek. Ons strategisch vlaggenschip is de IOCTA; het Internet Organised Crime Threat Assessment. In het najaar van 2015 is de tweede editie verschenen, in samenwerking met Interpol. Vanuit een opsporingsgerichte focus zijn ontwikkelingen, trends en bedreigingen in beeld gebracht. Afbeelding 1 laat zien wat de belangrijkste 'drivers' zijn voor de groei van cybercriminaliteit. Afbeelding 2 laat de belangrijkste trends zien.

Meer agressiviteit

Waar in de afgelopen jaren cybercriminaliteit veelal onder de oppervlakte bleef en op een 'stealth'-achtige wijze plaatsvond, is er nu sprake van een ware trendbreuk. Cybercriminaliteit wordt steeds agressiever. Dit is vooral te merken aan de openlijke dreiging met ransomware, het onverholen aankondigen van DDoS-attacks als een slachtoffer niet betaalt tot aan de veel openlijkere manier waarop seksuele gunsten worden afgedwongen. Vooral de eerste twee vormen van afpersing zijn een bewijs van de toegenomen betrokkenheid van de georganiseerde criminaliteit. Steeds vaker wordt daarbij gebruikgemaakt van een 'Cybercrime-as-a-Service'-model waarin alles te koop is en op afroep 'besteld' kan worden. Daarmee wordt de markt van cybercriminaliteit opengebroken voor een veel grotere groep van criminelen die niet noodzakelijk over uitgebreide kennis hoeven te beschikken.

Aanpak infrastructuur

In reactie op 'Cybercrime-as-a-service' heeft Europol de criminele businessmodellen in kaart gebracht. Een van de conclusies die daaruit kan worden getrokken, is dat de internationale opsporing in de nabije toekomst zich bij voorkeur moet richten op het aanpakken van criminele infrastructuren, zoals bullit proof hosting, money mules, laundering-faciliteiten en het aanbieden van anti-forensic tools. Dat deze aanpak kan slagen, blijkt uit het JCAT-samenwerkingsverband (Joint Cybercrime Action Taskforce) dat het afgelopen jaar bij EC3 is ontstaan. Een aantal Europese landen en partners als Australië en de Verenigde Staten vaardigen deskundigen af om gezamenlijk een zaak voor te bereiden. In een permanente JCAT-structuur wordt informatie verzameld en potentiële onderzoeken geïdentificeerd en gecoördineerd. De leiding daarvan ligt wisselend bij een van de lidstaten. In de tweede helft van 2015 heeft dat tot zeven grote succesvolle operaties geleid.

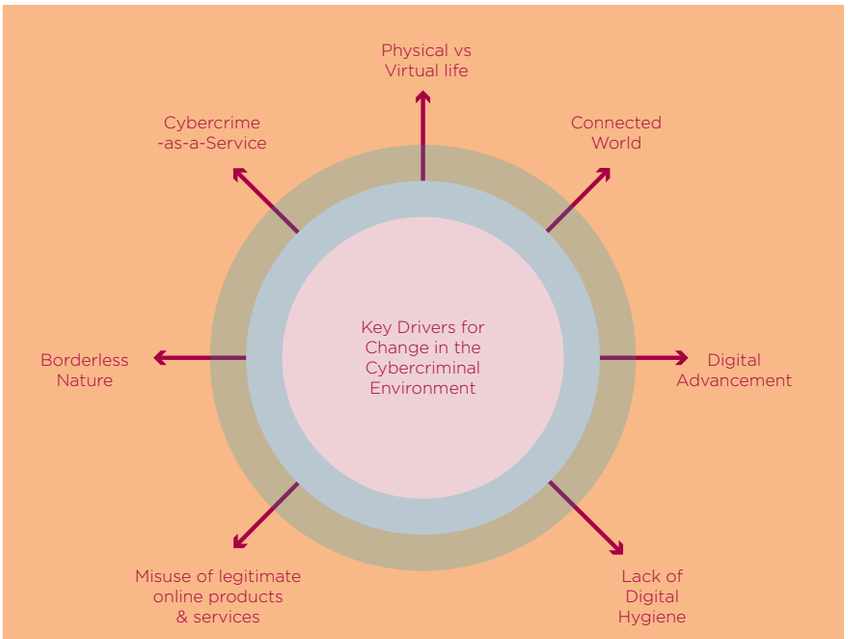
from a forensic perspective. Figure 1 illustrates the most important 'drivers' of the growth of cyber crime. Figure 2 shows the most important trends.

More aggressive

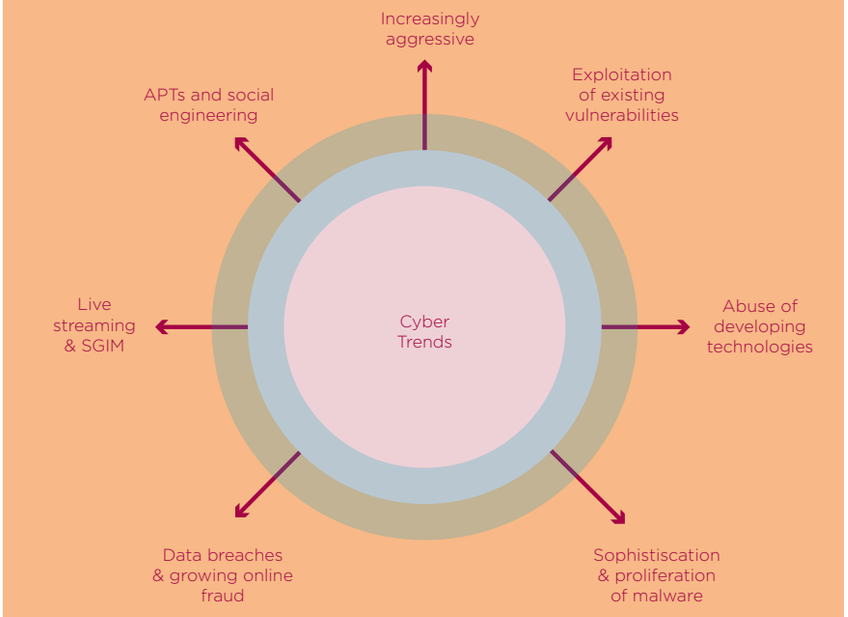
In previous years most cybercrime was below the surface and usually committed through 'stealth', but now there is a complete departure from that trend. Cybercrime is becoming more aggressive. Today we are confronted by blatant threats with ransomware, the undisguised announcement of DDOS attacks when a victim fails to pay up, and far more open methods of coercing sexual favours. The first two forms of extortion are evidence of the greater involvement of organised crime. We increasingly see the 'Cyber Crime-as-a-Service' model being deployed, where everything is for sale and can be 'ordered' on a call-up basis. This opens up the cybercrime market to a far larger group, because the perpetrators no longer need a huge amount of expertise.

Tackling the infrastructures

In response to 'Cyber Crime-as-a-service', Europol mapped out the various criminal business models. One of the conclusions that emerged from this was that in the immediate future it would be better for international investigations to concentrate more on tackling criminal infrastructures such as bulletproof hosting, money mules, laundering facilities and the provision of anti-forensic tools. We know this approach can succeed from the JCAT (Joint Cybercrime Action Taskforce) set up at EC3 last year. A number of European countries and other partners, including



Afbeelding 1 *figure 1*



Afbeelding 2 *figure 2*

Partnerschappen

Dankzij de oprichting van EC3 is er binnen Europol een platform ontstaan dat op het gebied van cybercrime vooruitgang boekt als het gaat om internationale samenwerking en partnerschappen met de private industrie. Zo is er bijvoorbeeld een sterke behoefte bij financiële dienstverleners en de internationale beveiligingsindustrie om afspraken te maken op Europees niveau. EC3 faciliteert dit. Inmiddels zijn er ruim dertig memoranda afgesloten voor strategische samenwerking en informatie-uitwisseling met de private industrie. De resultaten daarvan komen ter beschikking van de Europese (cyber)politiediensten in de vorm van regelmatige notificaties en producten zoals de Cyberbits-nieuwsbrief.

Proeftuin

De cyberwereld is dynamisch en de ontwikkelingen gaan razend snel. Het is daarmee een goede proeftuin voor andere vormen van (politie) samenwerking. Voor een langzame of stapsgewijze aanpak is hier geen ruimte. Het adagium 'Think Big, Act Big' is hier zeker van toepassing. Alleen wat mij betreft met een andere betekenis: Brave, Innovative and Grouped.

Australia and the United States, delegate experts to take part in the joint preparation of a case. Information is collected in a permanent JCAT structure and potential investigations identified and coordinated. The leadership switches from one member state to another. This led to the successful conclusion of seven major investigations in the second half of 2015.

Partnership

With the formation of EC3, a platform has been created inside Europol which is making good progress in the field of cybercrime when it comes to international cooperation and partnerships with private industry. There is a strong demand among financial service providers and the international security industry, for example, for agreements at the European level. EC3 helps to facilitate such agreements. More than thirty memoranda have been agreed to for strategic cooperation and exchanging information with private industry. The results are made available to the European (cyber) police in the form of regular announcements and publications such as the Cyberbits newsletter.

Test bed

The cyber-world is dynamic and new developments are taking place incredibly fast. This makes it an excellent test bed for other forms of (police) cooperation. There is no room for a gradual step-by-step approach. The old adage 'Think BIG, Act BIG' definitely applies here, whereby BIG (as far as I am concerned) also stands for 'Brave, Innovative & Grouped'.


Miranda Koopman

MARCEL KROM

new member of the Cyber Security Council

‘DON’T COMPETE WHEN IT COMES TO CYBER SECURITY’

Marcel Krom is sinds 2009 Chief Information Officer (CIO) bij PostNL. Als nieuwe voorzitter van het CIO Platform Nederland is hij in 2015 toegetreden tot de Cyber Security Raad. *Marcel Krom has been serving as Chief Information Officer (CIO) at PostNL since 2009. As the new chair of CIO Platform Netherlands, he joined the Cyber Security Council in 2015.*

Bij het CIO Platform Nederland zijn 120 organisaties aangesloten uit overheid en bedrijfsleven. Speelt cybersecurity binnen het platform een rol?

“Binnen het platform is een werkgroep informatiebeveiliging actief, die nadrukkelijk cybersecurity op de agenda heeft staan. Onze leden delen kennis op dit onderwerp, omdat we als CIO Platform de stelling innemen dat cybersecurity boven je eigen bedrijfsbelang uitstijgt. Je kunt dit niet alleen voor elkaar krijgen. Je hebt elkaar nodig. Iedereen heeft te maken met cyberissues. Kennis hierover is schaars en de investeringen zijn hoog. Daarom koppelen we leden die elkaar kunnen helpen aan elkaar. Iedereen heeft belang bij een veilig digitaal Nederland. Daarom moet je elkaar niet op dit onderwerp beconcurreren. Het CIO Platform gebruikt cybersecurity als samenbindend element, om met elkaar cyberdreigingen het hoofd te bieden.”

Waarom neemt u deel aan de Cyber Security Raad?

“De leden van het CIO Platform zijn overheden en bedrijven aan de vraagkant van de IT-markt. Als voorzitter breng ik onze kennis en ervaring in bij de Cyber Security Raad, omdat wij belang hebben bij een hoog niveau van cybersecurity in Nederland. Dat is het overstijgende belang van alle CSR-leden. Strategische aandacht voor cybersecurity is goed voor ons land, de economie en de businesscontinuïteit. Ontwikkelingen op dit vlak koppel ik terug binnen ons platform, zodat we met elkaar werken aan een hoger cyberveiligheidsniveau.”

CIO Platform Netherlands is composed of some 120 government and corporate organisations. Is cybersecurity addressed by the Platform?

“The Platform’s Information Security Committee expressly put cybersecurity on its agenda. Our members share knowledge on the subject, because we, as the CIO Platform, believe that the cybersecurity question exceeds the business interests of one’s own organisation. You cannot achieve cybersecurity on your own. You need each other. Everyone is affected by cyber issues. Knowledge is often lacking and investment costs are high. And that’s why we link members able to help each other out to one another. Everyone benefits from a secure digital realm. And that’s why you should not compete when it comes to cybersecurity. The CIO Platform considers cybersecurity to be a question bringing our members together, so we can form a united front against cyber threats.”

Why have you joined the Cyber Security Council?

“The CIO Platform members are all governmental bodies and businesses active on the demand side of the IT market. As Platform chair, I offer our knowledge and experience to the Cyber Security Council, as we all benefit from a high level of cybersecurity in the Netherlands. This interest is what connects all CSC members. Strategic attention to cybersecurity is beneficial to our country, to the economy and to business continuity. I then provide feedback on all developments in the field to the Platform, allowing us to all work together to improve the level of cybersecurity.”

By **Marcel Krom,** chair of CIO Platform Netherlands

Cybercrime bedreigt de bedrijfscontinuïteit. Als gevolg daarvan behoort cybersecurity tot de primaire verantwoordelijkheden van de board. Cybersecurity is géén IT-feestje alleen. Het gaat ook over het gedrag van medewerkers, want de meeste cyberincidenten worden door hen veroorzaakt. *Cybercrime threatens business continuity. Cyber security should therefore be a core board responsibility. Cyber security is not just about IT. It is also about staff conduct, for most cyber incidents are caused by staff.*

PROTECT THE CORPORATE TREASURES

Bestuurders van bedrijven en organisaties zullen meer dan nu het geval is cyberdreiging serieus moeten nemen. En najagen dat de organisatie zich bewust is van dit gevaar, zich wapent en verdedigingsstrategieën heeft als er toch iets gebeurt. De bedrijfscontinuïteit is een bestuurdersverantwoordelijkheid en die continuïteit wordt bedreigd. Zo zien we in toenemende mate DDoS-aanvallen, cryptoware en aanvallen die bekend staan onder de naam Advanced Persistent Threats.

Naast deze directe bedreiging van de bedrijfsvoering is er ook de indirecte dreiging van datalekken. Dit kan de concurrent versterken, de aandeelhouderswaarde doen dalen en reputatieschade opleveren. Verder treedt er in Nederland per 1 januari 2016 een nieuwe wet in werking, die grote boetes oplegt als datalekken niet tijdig worden gemeld en afgehandeld. Daarom is het zaak dat iedere board of directie cybersecurity hoog op de agenda heeft staan.

Bedrijfsschatten

Chief Information Officiers (CIO's) hebben de taak om in de board cyberdreigingen te delen en steun te verwerven voor de noodzakelijke maatregelen. Zij moeten aangeven wat de bedrijfsschatten zijn en hoe die te beveiligen. Cybersecurity is echter géén IT-feestje alleen. Het gaat namelijk niet alleen om het nemen van technische maatregelen, maar ook om bijvoorbeeld het trainen van medewerkers. Zo zien wij vooral spear phishing opkomen, waarbij medewerkers op de financiële afdeling worden verleid geld over te maken. Relaties en informatie die medewerkers vrijelijk delen op internet worden door de aanvallers geanalyseerd. Vervolgens sturen zij zeer betrouwbaar ogende e-mails de organisatie in. Het trainen en beschermen van de organisatie kost geld en het is aan de CIO om de noodzaak daarvan uit te leggen. Negeren is geen optie. Investeren in cybersecurity zou net zo normaal moeten zijn als het investeren in sloten op de deur. We maken ons op bestuurlijk niveau wel druk om fysieke toegangsaspecten, maar ondertussen kunnen de criminelen digitaal (vaak zeer) eenvoudig hun slag slaan. Daarnaast moet het denken over veiligheid een element zijn in de besluitvorming, door het hele organisatie heen. Dat kan alleen als bestuurders het goede voorbeeld geven.

Samenhangend Europees beleid

Op het gebied van cybersecurity moet het bedrijfsleven niet willen concurreren. De dreiging van kwaadwillenden is veel bedreigender dan de onderlinge concurrentie. Je kunt niet alleen het gevecht aangaan. Daar heb je elkaar

Managers of companies and organisations should take cyber threats more seriously than they do now, and work to make sure the organisation is well aware of the dangers, arms itself against them and has defence strategies in place should a threat materialise. Business continuity is a responsibility of the board. And this continuity is under threat. DDoS-attacks, cryptoware and so-called Advanced Persistent Threats become ever more prevalent. In addition to these direct threats to business operations, organisations are faced by the indirect threat of data leakage. Such leaks can strengthen the position of a competitor, cause a drop in shareholder value and damage the organisation's reputation. What's more, under a new Act, which will take effect in the Netherlands on 1 January 2016, heavy fines will be imposed for the failure to report and remedy data leaks in time. It is therefore of the essence that every board puts cyber security high on the agenda.

Corporate treasures

Chief Information Officers (CIOs) are charged with sharing cyber threats with the board and with gathering support for the implementation of necessary measures. They are to determine what the organisation's corporate treasures are and decide on how to secure and protect them. However, cyber security is not just an IT question. It is not just about taking technical measures, but also for example about educating staff. A prominent new threat is the

CYBERSECURITY HOORT THUIS IN DE BOARDROOM

CYBER SECURITY HAS A PLACE IN THE BOARDROOM


Miranda Koopman

voor nodig. Kennis is schaars en investeringen zijn hoog. Binnen CIO Platform Nederland delen we daarom informatie, dreigingen en best practices met elkaar. Cybersecurity verbindt ons en dat zou ik ook graag meer in Europa zien. Tussen bedrijven onderling, maar ook in samenhangend Europees beleid. Nu verschillen wetgeving, compliancy, privacy en organisatorische governance van land tot land. Dat brengt complexiteit en veel kosten met zich mee. Voor bedrijven die wereldwijd actief zijn, wordt het nog complexer. Het zou een grote stap vooruit zijn als de Europese landen wet- en regelgeving op het gebied van cybersecurity en privacy harmoniseren. Dan ontstaat er een 'level playing field' binnen Europa en kunnen we de concurrentie aan met Silicon Valley en ander innovatieve gebieden in de wereld. Dat komt de Europese economie ten goede.

so-called 'spear phishing' practice, which involves malignant parties conning finance department staff into transferring money. First, the attackers analyse the relations and information freely shared by these staff members on the Internet. Next, they send e-mails that appear to be legitimate to the organisation. Educating staff and protecting the organisation is a costly affair, and it is up to the CIO to explain why this isnecessary. Ignoring the threat is not an option. Investing in cyber security should be as common as investing in door locks. While boards are very well aware of the need to secure physical access, they allow cyber criminals to easily, and often even very easily, effect a digital break-in. Considering the security aspect of any decision should be part of the decision-making process, throughout all levels of the organisation. This is only possible when management sets a good example.

Coherent European policy

When it comes to cyber security, businesses should not want to compete with one another. The threat posed by malignant parties is bigger than the threat posed by competitors. You cannot win this fight alone. You need to work together. Knowledge is often lacking and investment costs are high. Therefore, within CIO Platform Netherlands, we share information, threats and best practices with one another. The cyber security question has brought us together, and I would like for this to happen at European level, too. Both in the shape of collaboration between companies and by a coherent European policy. Legislation, compliance, privacy and organisational governance differ from country to country. This results in complexity and high costs. Things are even more complex for globally active companies. If the European countries were able to harmonise their laws and regulations on cyber security and privacy, this would be a major step forward. This would lead to a level playing field in Europe, allowing us to compete with Silicon Valley and other innovation centres around the world, and that would boost the European economy.

By **David van Duren**, head of GFCE

GLOBAL FORUM ON CYBER EXPERTISE

Als spin-off van de Global Conference on Cyberspace (GCCS) 2015 in Den Haag is het Global Forum on Cyber Expertise (GFCE) opgericht. Het GFCE is een internationaal samenwerkingsverband waar het uitwisselen van expertise en wereldwijde best practices centraal staan. “Tijdens de GCCS bleek er een grote behoefte te bestaan aan een multi-stakeholderforum waarin landen, intergouvernementele organisaties en private organisaties samen aan capaciteitsbouw doen, waarbij experts van NGO’s, wetenschap en de technische gemeenschap worden betrokken”, vertelt David van Duren, hoofd GFCE Secretariaat dat gevestigd is in Den Haag. Inmiddels heeft de GFCE 48 leden, waaronder 34 landen en een aantal grote bedrijven zoals HP, Cisco en Microsoft. Naast dat de deelnemers aan de GFCE binnen het forum praktische en bruikbare kennis opdoen om de eigen cybercapaciteiten te versterken, dient het GFCE ook een hoger doel: het verder brengen van de wereldgemeenschap als het gaat om cybercapaciteitsopbouw. Zowel op het gebied van het tegengaan van dreigingen als het creëren van kansen. “Als secretariaat zorgen wij voor de verbinding tussen leden, faciliteren we samenwerkingsprocessen en internationale bijeenkomsten. Uitwisseling van kennis en expertise in een transparante omgeving is een van onze uitgangspunten.”

Awareness en CSIRT Maturity

Het GFCE focust op een aantal thema’s, mede gebaseerd op advies van de Cyber Security Raad. Dat zijn: cybersecurity, cybercrime, e-governance en data-protectie. Binnen deze thema’s zoeken deelnemende leden elkaar op. Ze richten een werkgroep op en maken een werkprogramma, dat vervolgens wordt uitgevoerd. “Op dit moment zijn er tien werkgroepen actief. Nederland is bijvoorbeeld de trekker van de werkgroep ‘Awareness’ en ‘CSIRT Maturity’.”

Meer informatie over de GFCE is te vinden op www.thegfce.com.

The Global Forum on Cyber Expertise (GFCE) was founded as a spin-off of the Global Conference on Cyberspace (GCCS) 2015 in The Hague. The GFCE is an international partnership whose central purpose is to promote the exchange of expertise and worldwide best practices. “During the GCCS it became apparent that there was a real need for a multi-stakeholder forum in which countries, intergovernmental organisations and private organisations can work together to build capacity and experts from NGOs and from the scientific and technical communities would also be involved”, says David van Duren, head of the GFCE Secretariat based in The Hague. Today the GFCE has 48 members, including 34 countries and numerous business concerns such as HP, Cisco and Microsoft. Apart from allowing participants to acquire practical and useful knowledge inside the forum to strengthen their own cyber capacities, the GFCE also serves a higher purpose: to help the world community as a whole to build its cyber capacity. Not only to combat threats but also to create opportunities. “The secretariat is responsible for connecting its members and facilitating collaborative processes and international conferences. The exchange of knowledge and expertise in a transparent environment is one of our fundamental principles.”

Awareness and CSIRT maturity

The GFCE focuses on a number of special themes, partly on the basis of advice from the Cyber Security Council. Those themes are: cyber security, cyber crime, e-governance and data protection. The participating members seek one another out within the context of these themes. They set up work groups and prepare programmes, which they then proceed to execute. “At present there are ten initiatives under way (active work groups). The Netherlands for example set up the work groups ‘Awareness’ and ‘CSIRT maturity’.

For more information about the GFCE see: www.thegfce.com.


Peter van Es

By **Tineke Netelenbos**, Chairman ECP

De Europese Unie heeft in elke lidstaat een 'digital champion'. Dit is een invloedrijk persoon vanuit overheid, wetenschap, bedrijfsleven of politiek die aangewezen is door de nationale regering om de Europese digitale agenda in de betreffende lidstaat uit te dragen. De 'champions' zorgen ervoor dat meer politieke discussie op nationaal niveau gevoerd wordt, zodat hun regering digitaal beleid maakt dat past bij de EU-agenda. *Each European Union Member State has its own 'digital champion', an influential individual from the world of government, academia, business or politics designated by the national government to promote the European digital agenda in that Member State. These 'champions' strive to promote political debate on at a national level and, thereby, to have their governments adopt policies in line with the EU agenda.*

EU DIGITAL CHAMPIONS ENDEAVOUR TO CREATE A DIGITAL SINGLE MARKET

Speerpunt van de 'champions' is onder andere een digital single market in Europa. Dit past bij de EU-cyberstrategie om internetgebruik en internetdiensten tussen Europese landen te liberaliseren en economische barrières te verwijderen. Ook thema's als interoperabiliteit, standaarden, e-skills, onderzoek en innovatie staan op de agenda. Tineke Netelenbos is lid van de Cyber Security Raad en 'digital champion' voor Nederland. Zij vertelt dat Nederland op de vierde plaats staat van de digital economy and society index. Deze index geeft onder andere aan hoeveel connectiviteit en internetgebruik er in een land is. "Nederland is binnen Europa een frontrunner, die andere landen kan helpen." Op de nationale agenda van Netelenbos staan onderwerpen als e-skills, onderwijs en internet-(cyber)security.

Gelijke digitale kansen

De 'digital champions' beloven in hun joint mission statement dat hun inzet gericht is op gelijke kansen voor iedere Europeaan in de digitale toekomst. Daarom zetten zij zich er voor in dat iedere EU-burger toegang heeft tot de digitale wereld, waarbij zij gebruik maken van een open en veilig internet. Netelenbos: "Het werk van een 'champion' is nooit af, want de ontwikkelingen gaan razendsnel. Er blijft genoeg werk aan de winkel, om Europa nog meer cybersecure te maken."

One focal point all champions share is the creation of a European digital single market. This is in line with the EU Cyber Security Strategy to liberalise internet use and internet services between the various European countries and to remove economic barriers. Themes like interoperability, standards, e-skills, research and innovation also have a place on the agenda. Tineke Netelenbos is a member of the Cyber Security Council and the digital champion of the Netherlands. She states that the Netherlands are in fourth place on the digital economy and society index. This index lists dimensions like the connectivity and use of the Internet within a country. "The Netherlands is a frontrunner within Europe, able to help out other countries." Netelenbos's national agenda includes themes like e-skills, education and internet (cyber) security.

Equal digital opportunities

In their joint mission statement, the digital champions promise to strive to realise equal opportunities in the digital future for every European. They will therefore strive to have every EU citizen have access to the digital society and be able to use an open and safe Internet. Netelenbos: "A champion's work is never finished, as matters develop with lightning speed. A lot of work is still to be done to make Europe ever more cybersecure."

Jasper Rietman

By **Steve Purser**, Head of Core Operations Department at ENISA

ENISA is een EU-agentschap met de opdracht om EU-instellingen en EU-lidstaten te helpen bij het verbeteren van de 'netwerk- en informatiebeveiliging' (NIB) in de hele EU. *ENISA is an EU agency with a mandate to assist the EU institutions and the EU member states in improving the state of 'network & information security' (NIS) throughout the EU.*

EUROPEAN UNION NETWORK AND INFORMATION SECURITY AGENCY (ENISA)

Omdat NIB voor een groot deel synoniem is aan cybersecurity, is onze opdracht erg breed. ENISA lost deze kwestie op verschillende manieren op:

- door zich te richten op werk dat niet ook ergens anders gedaan wordt;
- door samen te werken met deskundigen in de lidstaten en de private sector;
- door waar mogelijk gebruik te maken van synergieën en gemeenschappelijke doelen.

Vanwege onze zeer beperkte middelen is het tweede punt essentieel voor onze werkwijze. Door samen met en via andere operationele gemeenschappen te werken, zorgen we voor schaalbaarheid en betrokkenheid bij het eindproduct.

Incidentenverslag

Ieder jaar brengen we een incidentenverslag uit. De belangrijkste bevindingen van het incidentenverslag 2014 bevestigen de trend die ENISA de afgelopen drie jaar benadrukt heeft:

Since NIS is largely synonymous with cyber security, our mandate is very broad and ENISA resolves this issue in several ways:

- by focusing on work which is not being done elsewhere,
- by working together with experts in the member states and private sector,
- by exploiting synergies and common goals wherever possible.
- Because of our very limited resources, the second point is a critical component of our operational model. By working with, and through, other operational communities we achieve scalability and help ensure 'buy in' to the final product.

Incident Report

- Every year we publish an annual incident report. The main findings of the 2014 Annual Incident report confirm the trend that ENISA has highlighted over the last three years:
- Technical failures cause most outages: 65% of the reported incidents were caused by technical failures, mainly software bugs and hardware failures affecting switches and routers.
- Faulty software changes and updates have most impact: incidents caused by human errors and particularly faulty software changes and updates had most impact in terms of users impacted in combination with the duration of the incidents.

Role of standards

Standards play an important role in helping organizations to ensure an appropriate level of security for their operations. However, standards are only one of a number of mechanisms that are used in this way and it is key to use standards sensibly in collaboration with other mechanisms. These range from high-level policy statements and strategy documents, well documented processes and procedures, suitable use of 'good practice' and awareness/training initiatives for staff.

STANDAARDEN SPELEN EEN BELANGRIJKE ROL BIJ HET VINDEN VAN EEN GEPAST VEILIGHEIDSNIVEAU

STANDARDS PLAY AN IMPORTANT ROLE TO ENSURE AN APPROPRIATE LEVEL OF SECURITY

- Technische gebreken veroorzaken de meeste storingen: 65% van de gemelde incidenten worden veroorzaakt door technische gebreken, met name softwarefouten en hardwaregebreken die schakelaars en routers treffen.
- Ondeugdelijke softwarewijzigingen en updates hebben de meeste impact: incidenten die veroorzaakt worden door menselijke fouten en in het bijzonder ondeugdelijke softwarewijzigingen en updates hebben de meeste impact wat betreft het aantal getroffen gebruikers, in combinatie met de duur van de incidenten.

Rol van standaarden

Standaarden spelen een belangrijke rol bij het helpen van organisaties om te zorgen voor een gepast veiligheidsniveau voor hun activiteiten. Standaarden zijn echter slechts één van de mechanismen die hiervoor gebruikt worden en het is essentieel dat deze verstandig gebruikt worden in combinatie met andere mechanismen. Deze variëren van beleidsverklaringen en strategieën van hoog niveau tot goed vastgelegde processen en procedures, gepast gebruikt van 'good practices' en bewustwordings- en trainingsinitiatieven voor personeel.
Veiligheidsstandaarden komen vaak uit verschillende bronnen en kunnen gebaseerd zijn op verschillende veiligheidsmodellen. Het is belangrijk om standaarden zorgvuldig te kiezen. Zodat consequent handelen op het gebied van cybersecurity mogelijk wordt.

Het internet der dingen

Een van de belangrijkste veiligheidskwesties die verband houden met het internet der dingen is schaalbaarheid. Het is een gigantische uitdaging om een veiligheidskader voor het beschermen van miljoenen verspreide objecten in te stellen, te behouden en te beheren. Op dit vlak is er nog geen oplossing en zijn er nog geen implementatiemodellen waarvoor draagvlak is.
Een andere kwestie is de context waarin een apparaat functioneert. Dat heeft namelijk fundamentele gevolgen voor het te kiezen veiligheidsmodel. Een gebrekkige digitale thermometer in huis heeft maar beperkte consequenties, terwijl dit voor vervoer of in een industriële omgeving met controlesystemen wel een probleem kan zijn. Eigendom en zeggenschap vormen nog weer een kwestie. Dient de veiligheid van verspreide objecten eigendom te zijn en beheerd te worden door de gebruiker, de leverancier, een derde of een combinatie hiervan? Er is waarschijnlijk niet één antwoord op deze vraag, omdat er verschillende veiligheidsmodellen nodig zijn voor verschillende combinaties van objecten en omgevingen.
En zo zijn er nog meer kwesties te noemen. Om verder te komen op dit onderwerp werkt ENISA samen met de juiste deskundigen voor het definiëren van de operationele implementatieaanpak die het antwoord biedt op bovenstaande vragen. Deze ervaring kan vervolgens gebruikt worden om beleid en strategieën op EU-niveau te definiëren.

Another challenge is consistency. Security standards often originate from different sources and may be based upon different security models. It is important to choose collections of standards carefully.

Internet of Things

One of the main security issues related to Internet of Things is one of scalability. Establishing, maintaining and administering a security framework to protect millions of distributed objects is a huge challenge and is as yet unsolved in terms of agreed implementation models.
A second issue is that of context. The context in which a device or application executes has fundamental consequences for the appropriate security model. For example: a thermometer that malfunctions in a home environment will probably have limited consequences, but this might not be the case in a public transport or industrial control system.
Another issue is that of ownership and control. Should the security of distributed objects be owned and administered by the user, the supplier, a third party or a combination of these? There is probably no single answer to this question as different object/environment combinations will require different security models.

ICT-systemen hebben een al maar groter wordende invloed op ons leven. Als in deze systemen iets mis gaat, kan dat mensenlevens in gevaar brengen. “Dat de ICT’er zijn werk goed doet, is net zo belangrijk geworden als bij een arts of een accountant”, vindt Leon Strous, president van de International Federation for Information Processing (IFIP), de wereldwijde koepel van nationale ICT-verenigingen waaronder het NGI-NGN in Nederland. *“IT systems have an increasingly great influence on our life. When something goes wrong in these systems this may endanger people’s lives. IT workers doing their work well is just as important as doctors or accountants doing their work well”, according to Leon Strous, President of the International Federation for Information Processing (IFIP), the global umbrella organisation of national IT associations.*

PROFESSIONAL CODE HELPS IT WORKER WITH ETHICAL DILEMMAS

De ontwikkelingen in de sector gaan razendsnel. Steeds meer apparaten worden met elkaar verbonden via internet. Consumenten en bedrijven willen minder afhankelijk zijn van hun eigen technische infrastructuur; daardoor neemt de vraag naar diensten als werken in de cloud en software-as-a-service enorm toe. Ook de toenemende personalisering van systemen is een belangrijke ontwikkeling. Denk aan wearables die de gezondheid meten en daarover data bijhouden. Veel gebruikers willen deze informatie graag delen.

Complex samenspel

Strous: “Al deze ontwikkelingen zorgen ervoor dat de beschikbaarheid, de veiligheid en betrouwbaarheid van de systemen steeds belangrijker worden. Tegelijkertijd zien we dat de wet- en regelgeving achterloopt. Het is niet altijd duidelijk wat wel en niet mag, welke (persoonlijke) data waarvoor gebruikt mogen worden en welke ICT-diensten van zo’n vitaal belang zijn dat ze aan extra eisen moeten voldoen.” Bij cybersecurity gaat het volgens Strous om een complex samenspel van bedrijven, overheden en andere spelers, zoals de beroepsverenigingen, die elk hun eigen verantwoordelijkheid hebben. “We moeten ons daarbij niet alleen richten op grote bedrijven, maar juist ook op de kleinere. Ook Facebook is ooit klein begonnen. Als we met elkaar afspraken willen maken en zaken willen reguleren, dan is het slimmer om er snel bij te zijn.’

The developments in the IT sector are moving very fast. An increasing number of devices are connected with each other through the internet. Consumers and companies want to be less dependent on their own technical infrastructure. This is why the demand for services such as working in the cloud and software-as-a-service is increasing substantially. The increasing personalisation of systems is an important development. For example, wearables that measure and record data about health. Many users like to share this information.

Complex interplay

Strous: “All these developments mean that the availability, security and reliability of the systems are becoming increasingly important. At the same time we see that legislation and regulations lag behind. It is not always clear what is allowed and what is not, which (personal) data can be used and for what purpose and which IT services are so important that they have to comply with extra requirements.” According to Strous, cybersecurity involves a complex interplay of companies, authorities and other players, such as professional associations, each of which have their own responsibility. “We should hereby not only focus on large companies, but in particular also on smaller companies. Facebook also used to be a small company. When we make arrangements with each other and want to regulate matters, it is smarter to act quickly.”

Listing competences

Strous observes that the lack of IT workers is becoming increasingly acute. For example, Australia gets all its IT staff from Asia, mainly from India. In Europe it is estimated that the shortage of IT workers will exceed 800,000 in 2020. Many companies subcontract their IT completely to companies in other parts of the world. Because they can save costs, but also because of the availability of staff. “This is why it is important that IT jobs can be compared better on an international level”, according to Strous. “So that organisations exactly know what the value is of an IT professional. Whether he comes from Europe, Asia or the USA. The ‘e-competence framework’ has been developed for

DE WET- EN REGELGEVING LOOPT ACHTER

THE LEGISLATION AND REGULATIONS LAG BEHIND

Competenties in kaart

Strous signaleert dat het tekort aan ICT'ers steeds nijpender wordt. Australië haalt bijvoorbeeld al ICT-personeel uit Azië, voornamelijk uit India. In Europa is het tekort geraamd op ruim 800.000 mensen in 2020. Veel bedrijven besteden hun ICT integraal uit aan bedrijven in andere werelddelen. Vanwege de kosten, maar ook vanwege de beschikbaarheid van personeel. "Daarom is het belangrijk dat ICT-functies wereldwijd beter te vergelijken zijn", meent Strous. "Zodat organisaties precies weten wat ze hebben aan een ICT-professional. Of die nou uit Europa, Azië of de VS komt. In Europa is hiervoor het 'e-competence framework' ontwikkeld. Dit raamwerk beschrijft de vaardigheden en het beroepsniveau van een ICT-professional. In andere werelddelen zijn er andere indelingen. Het mooiste zou zijn als we ze op termijn in elkaar kunnen schuiven."

Gerommel met software

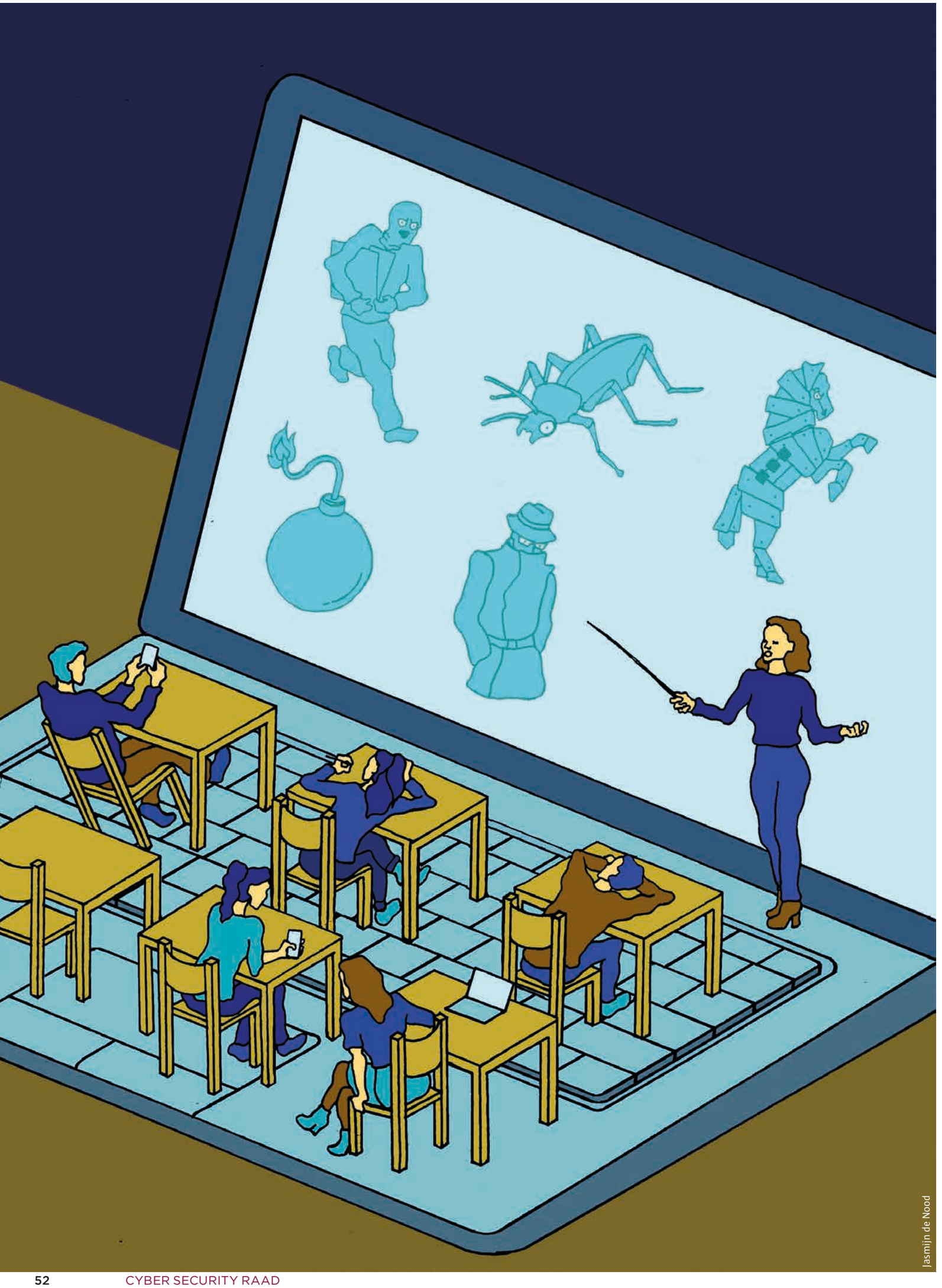
IFIP werkt aan de professionalisering van het ICT-vak. Daarbij gaat het niet alleen om competenties, maar ook om beroepsethiek. Strous: "Natuurlijk zijn de beslissers in een organisatie eindverantwoordelijk, maar wat is onze rol als ICT'er? Wat doen we bijvoorbeeld als ons bedrijf om commerciële redenen te snel een product in de markt wil zetten? De Global Industry Council van IFIP heeft een visie uitgebracht die daar op ingaat." In dit kader bevordert IFIP de ontwikkeling van beroepscodes voor ICT'ers, vergelijkbaar met de codes van bijvoorbeeld registeraccountants. "Dat geeft je als ICT'er bij ethische dilemma's een steviger onderhandelingspositie, naar je baas of naar je opdrachtgever. Vanuit IFIP zouden we graag zien dat er wereldwijd een uniform systeem komt."

this purpose in Europe. This framework describes the skills and professional level of an IT professional. In other parts of the world there are other classifications. It would be fantastic if we could create one system in the future."

Professional code

IFIP is working on the professionalization of the IT profession. This does not only involve competences, but also professional ethics. Strous: "Of course the decision-makers in an organisation have the final responsibility, but what is our role as an IT worker? What do we do, for example, when our company wants to market a product too quickly for commercial reasons? The Global Industry Council of IFIP has published its views on this." In this respect IFIP promotes the development of professional codes for IT workers, comparable with the codes of, for example, chartered accountants. "This offers you a stronger negotiation position as an IT worker in the event of ethical dilemmas, with regard to your boss or your client. At IFIP we would like to see one international uniform professional code."

Foto credits?



Jasmijn de Nood

By **Leo Faber**,
Deputy Secretary-General of Luxembourg's Ministry of Foreign Affairs and Chair of the EU

Leo Faber, plaatsvervangend Secretaris-Generaal van het ministerie van Buitenlandse Zaken van Luxemburg en voorzitter van de EU-werkgroep inzake cyberkwesties, deelt zijn perspectief op het bouwen van een open, vrij en veilig internet. Met de juiste vaardigheden, infrastructuur en beleidsprioriteiten kan de Europese Unie een dynamische digitale interne markt ontwikkelen die in het belang is van al haar burgers. Als bilaterale partners en opeenvolgende voorzitters van de EU kunnen Luxemburg en Nederland de weg wijzen. *Leo Faber, Deputy Secretary-General of Luxembourg's Ministry of Foreign Affairs and Chair of the EU Cyber issues working group, shares his perspective on building an open, free and secure internet. With the right skills, infrastructure and policy priorities, the European Union can develop a dynamic Digital Single Market in the interest of all its citizens. As bilateral partners and as successive EU Presidencies, Luxembourg and the Netherlands can show the way.*

E-SKILLS INDISPENSABLE FOR A DIGITAL SINGLE MARKET

In de huidige hyper-verbonden wereld gaat cybersecurity iedereen aan. ICT-vaardigheden, van basisvaardigheden voor het gebruik van computers tot geavanceerde codering, zijn onmisbaar geworden voor de huidige en toekomstige beroepsbevolking. Als vorige voorzitter van de Raad van de Europese Unie heeft Luxemburg als doel gehad om bij te dragen aan het opbouwen van een dynamische digital single market op basis van een open, vrij en veilig internet en standvastige toewijding aan het respecteren van de mensenrechten, zowel online als offline. Digitaal werken is gunstig voor alle sectoren van de economie en biedt talloze mogelijkheden om de basis te leggen voor een echte informatie-economie en kennismaatschappij. Het beschermen van de mensenrechten en het behouden van de fundamentele vrijheden is essentieel om ervoor te zorgen dat iedereen profiteert.

Europese ICT-hub

ICT is een van de snelst groeiende sectoren van de Luxemburgse economie en bevindt zich in het centrum van onze strategie voor economische diversificatie. Doordat ons land zo klein is, zijn een goede breedbanddekking en toegang tot draadloos internet gemakkelijk te realiseren. Dankzij de consensus onder vele belanghebbenden over het belang van ICT-vaardigheden, zijn deze opgenomen in het vakaanbod op scholen; de beroepsbevolking maakt ze zich eigen door e-learning en levenslang leren. Met zijn eersteklas infrastructuur, bekwame beroepsbevolking en geïntegreerde strategie wil Luxemburg zijn reputatie als eerste hub voor ICT-diensten in

In today's hyper-connected world, cyber security is everybody's business. ICT skills, from basic computer literacy to advanced coding, have become indispensable for today's and tomorrow's workforce. As the former President of the Council of the European Union, Luxembourg aimed to contribute to building a dynamic digital single market, based on an open, free and secure internet and on an unwavering commitment to uphold human rights, on- and offline. Going digital benefits all sectors of the economy and presents numerous opportunities, laying the foundations for a real information economy and knowledge-based society. Protecting human rights and preserving fundamental freedoms is indispensable to make everyone benefit.

European ICT hub

ICT is one of the fastest-growing sectors of Luxembourg's economy and at the heart of our economic diversification strategy. The small size of our country allows for easy coverage with broadband and wireless internet access. A multi-stakeholder consensus on the importance of ICT skills has allowed their integration into school curricula; they're being picked up by the workforce through eLearning and lifelong learning. With its top-notch infrastructure, skilled workforce and integrated strategy, Luxembourg is aiming to consolidate its reputation as a premier hub for ICT services in Europe. To this end, the

CYBERSECURITY GAAT IEDEREEN AAN

CYBER SECURITY IS EVERYBODY'S BUSINESS

Europa verstevigen. Hiervoor is vorig jaar het platform 'Digital Lëtzebuerg' gelanceerd, waarin verschillende publieke en private belanghebbenden samengebracht worden rond een uitgebreide strategie voor de sector.

E-skills in Europa

Innovatie begint met mensen. Voor een digitale interne markt zijn niet alleen consumenten nodig die handig zijn met internet, maar ook mensen die kunnen creëren en daarvoor over de juiste vaardigheden beschikken. Als Europa de vruchten wil plukken van een dynamische digital single market die goede banen creëert en ondersteunt, is het essentieel om ICT-vaardigheden op te nemen in formeel en niet-formeel onderwijs. Het goede nieuws: het is nog nooit zo gemakkelijk geweest om nieuwe vaardigheden te leren en dat geldt des te meer voor ICT-vaardigheden. Voorheen werd informatie als handelswaar gezien, maar nu heb je gratis toegang tot een enorme schat aan informatie en kun je jezelf nuttige vaardigheden aanleren. Als je in je vrije tijd op een app op je mobiele telefoon kunt leren coderen, ben je als consument een stap dichter bij het creëren van iets nieuws. Er zijn talloze mogelijkheden waarin de publieke en private sector hierin kunnen samenwerken: tijdens ons voorzitterschap hebben we ons gericht op het bouwen van bruggen tussen de publieke en private sector en tussen de academische wereld en de maatschappij. Door de onderlinge afhankelijkheid van de wereldeconomie in de 21e eeuw is het belangrijk dat wij deze inspanningen samen blijven verrichten.

'Digital Lëtzebuerg' platform was launched last year, bringing together different public and private stakeholders around a comprehensive strategy for the sector.

E-skills in Europe

Innovation starts with people. A digital single market doesn't just require internet-savvy consumers, but also creators, who bring the right skill-set to the table. Integrating E-skills throughout formal, informal and non-formal education is indispensable if Europe wants to reap the benefits of a dynamic digital single market that creates and sustains quality jobs. The good news: it has never been easier to pick up new skills and that's doubly true for e-skills: while information used to be treated as a commodity, you now have access to a huge amount of knowledge – for free – and can teach yourself useful skills. If you can learn to code in your spare time on an app on your mobile phone, you're one step closer as a consumer to become a creator. There are ample opportunities for the public and private sectors to work together here: during our Presidency, we focused on building bridges between public and private sector, as well as with academia and civil society. The interdependent nature of the global economy in the 21st century means that this is an endeavour that we must undertake together.

By **Alexander Seger,** Executive Secretary, Cybercrime Convention Committee and Head of Cybercrime Programme Office of the Council of Europe (C-PROC).

Het Verdrag inzake cybercrime is in 2001 in Boedapest ter ondertekening opengesteld en is sindsdien de wereldwijde norm voor wetgeving inzake cybercrime geworden. De relevantie van dit verdrag voor wereldwijde internationale samenwerking op het gebied van cybercrime en elektronische bewijsvoering neemt nog steeds toe. Het Verdrag wordt ondersteund door follow-upmechanismen en programma's voor capaciteitsopbouw. De vraag is hoe nieuwe uitdagingen, zoals toegang tot elektronisch bewijs in de cloud, aangepakt kunnen worden. *The Convention on Cybercrime was opened for signature in Budapest in 2001 and has since become the global norm for cybercrime legislation. Its relevance as a framework for international cooperation on cybercrime and electronic evidence worldwide keeps increasing. The Convention is backed up by a follow up mechanism and capacity building programmes. The question is how new challenges can be addressed such as access to electronic evidence in the cloud.*

INTERNATIONAL COOPERATION ON CYBERCRIME:

THE BUDAPEST CONVENTION AS A FRAMEWORK

Het Verdrag van Boedapest is een strafrechtelijk verdrag en vraagt van partijen om:

- een lijst op te stellen van strafbare cyberaanvallen met behulp van of tegen specifieke computers;
- rechtshandhavende instanties bevoegdheden te verlenen voor het bewaren, doorzoeken, in beslag nemen of onderscheppen van gespecificeerde computergegevens in specifieke strafrechtelijke procedures en in verband met strafbare feiten;
- deze bevoegdheden te beperken middels voorwaarden en waarborgen;
- politieel en justitieel efficiënt samen te werken, onder andere door middel van een 24/7-netwerk van contactpersonen.

The Budapest Convention is a criminal justice treaty which requires Parties to:

- criminalise a list offences against and by means of computers
- provide law enforcement with the powers to preserve, search, seize or intercept specified computer data in specific criminal investigations and in relation any criminal offence
- limit such powers through conditions and safeguards
- engage in efficient international police-to-police and judicial cooperation, including through a 24/7 network of contact points.

Although prepared by the Council of Europe, the participation in the negotiations by Canada, Japan, South Africa and the USA showed from the outset that this was to be an open treaty with a global ambition. Currently, 66 States are either parties (the latest being Canada and Sri Lanka), signatories or have been invited to accede. At least twice that number have used it as a guideline for domestic legislation. These numbers are increasing.

Effective framework

The Budapest Convention has become an effective international framework for cooperation on cybercrime and electronic evidence, in particular, because it is backed up by:

- the Cybercrime Convention Committee (T-CY) comprising the Parties and observer States as well as European Commission, EUROPOL, EUROJUST, INTERPOL, the UN Office on Drugs and Crime and other relevant organisations. The Committee assesses implementation of the treaty in practice, adopts Guidance Notes and may also prepare additional Protocols to the Convention.

Hoewel het verdrag is opgesteld door de Raad van Europa, liet de deelname van Canada, Japan, Zuid-Afrika en de VS aan de onderhandelingen zien dat dit een open verdrag met een wereldwijde ambitie moest worden. Op dit moment zijn 66 landen betrokken bij het verdrag (met als recentste Canada en Sri Lanka) als ondertekenaar of potentiële kandidaat om te ondertekenen. Minimaal twee keer zoveel landen hebben het als richtlijn voor hun binnenlandse wetgeving gebruikt. En deze aantallen blijven stijgen.

Effectief kader

Het Verdrag van Boedapest is een effectief internationaal kader geworden voor samenwerking op het gebied van cybercrime en elektronische bewijsvoering. Dit heeft vooral te maken met de ondersteuning door:

- het Cybercrime Convention Committee (T-CY) dat onder andere bestaat uit lidstaten, Europese Commissie, Europol, EuroJust, Interpol, Bureau van de Verenigde Naties voor drugs- en misdaadbestrijding en andere relevante organisaties. Het comité beoordeelt de imple-

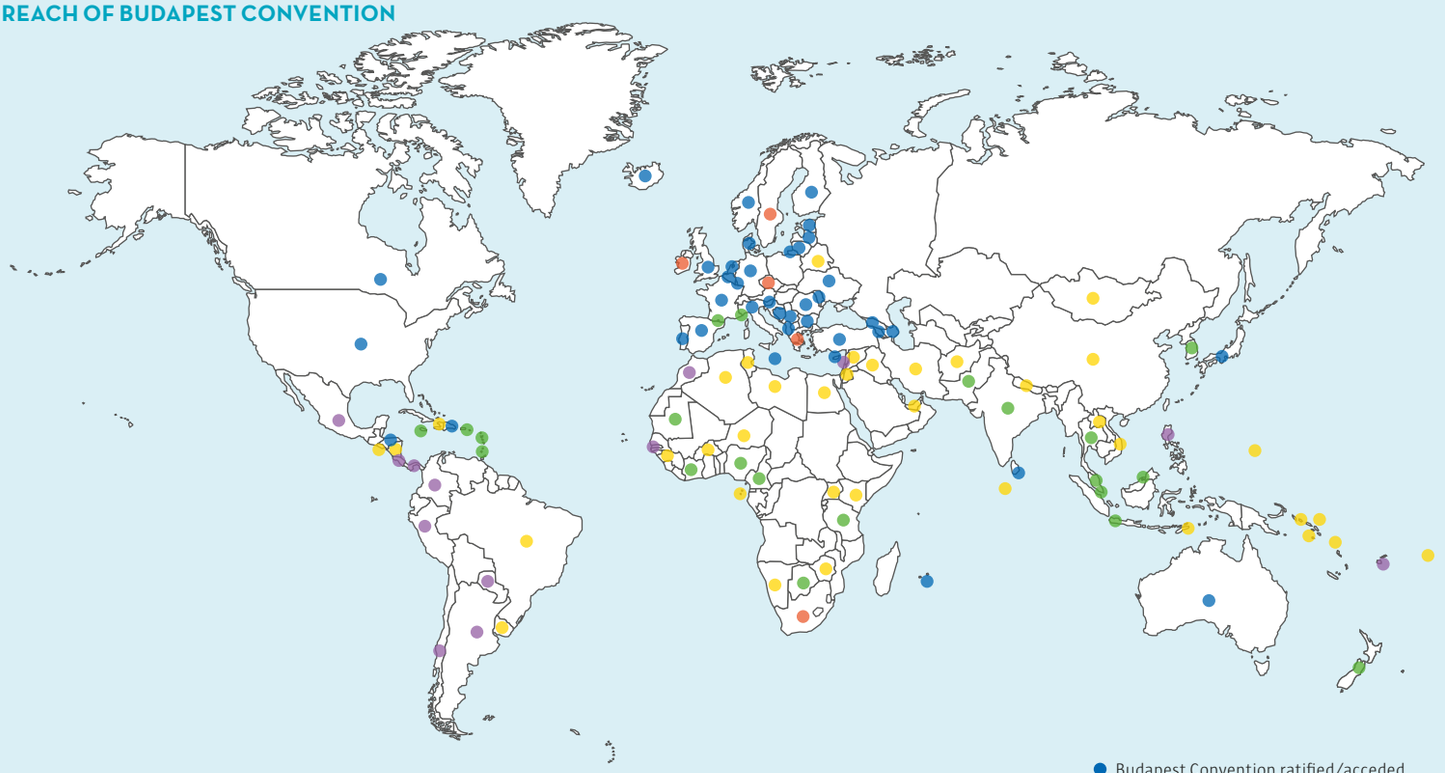
---

- capacity building programmes to assist countries worldwide in the strengthening of legislation, training of police, judges and prosecutors, public/private and international cooperation. Since April 2014, these programmes are implemented through the Cybercrime Programme Office of the Council of Europe (C-PROC) in Romania. The purpose of C-PROC is to support capacity building on cybercrime worldwide.

New challenges

With the evolution not only of the threat landscape but also technology, new challenges emerge. For example, the jurisdiction of criminal justice authorities is very much tied to the principle of territoriality. However, in the context of cloud computing, data – and thus evidence – may be stored in or flow between foreign, multiple or unknown jurisdictions and be held temporarily or in parts by multiple layers of service providers. What laws apply and to whom to address a request for mutual legal assistance? In the absence of international agreements, government increasingly take unilateral action to access data in the cloud. This is leading to a jungle of approaches that entail considerable risks to state-to-state relations and to the rights of individuals. The Cybercrime Convention

REACH OF BUDAPEST CONVENTION



Budapest Convention ratified/acceded	47
Signed	7
Invited to acceded	12
Total	66
Other states with laws/draft laws largely in line with Budapest Convention	20
Further states drawing on Budapest Convention for Legislation	45+

mentatie van het verdrag in de praktijk, stelt richtlijnen en aanvullende protocollen vast;

- programma's voor capaciteitsopbouw om landen over de hele wereld te helpen bij het verstevigen van de wetgeving, de training van politie, rechters en aanklagers, en de publiek-private en internationale samenwerking. Sinds april 2014 worden deze programma's geïmplementeerd door het Cybercrime Programme Office van de Raad van Europa (C-PROC) in Roemenië. Het doel van C-PROC is het ondersteunen van de wereldwijde capaciteitsopbouw tegen cybercrime.

Nieuwe uitdagingen

Doordat niet alleen de dreigingen, maar ook de technologie zich ontwikkelt, komen we voor nieuwe uitdagingen te staan. Zo wordt de jurisdictie van strafrechtelijke instanties ingeperkt door landsgrenzen. Echter, in de context van cloud computing kunnen data (en dus ook bewijzen) opgeslagen worden in of verplaatst worden tussen verschillende landen met verschillende of onbekende juridische regimes en verschillende serviceproviders. De vraag is dan welke wetten er gelden en aan wie een verzoek om wederzijdse rechtshulp gericht moet worden. Door het ontbreken van internationale overeenkomsten ondernemen overheden steeds vaker eenzijdige acties om toegang te krijgen tot data in de cloud. Dit leidt tot een oerwoud van verschillende benaderingen die aanzienlijke risico's met zich meebrengen voor de relatie tussen landen onderling en voor de rechten van burgers. Het Cybercrime Convention Committee heeft een 'werkgroep voor bewijsvoering in de cloud' opgericht die tot uitvoerbare oplossingen moet zien te komen. Denk hierbij aan het beter gebruikmaken van bestaande bepalingen uit het Verdrag van Boedapest en aanvullende protocollen. In de loop van 2016 zullen hiervoor specifieke voorstellen gedaan worden.

Het sluiten van aanvullende overeenkomsten is moeilijk, maar wel noodzakelijk. Het Verdrag van Boedapest is daarvoor het best geschikt als kader, om zo nieuwe oplossingen mogelijk te maken.

Committee recently established a 'Cloud Evidence Working Group' to identify feasible answers. Solutions may include better use of already existing provisions of the Budapest Convention or additional Protocols. Specific proposals should become available in the course of 2016.

Additional agreements are difficult to achieve but necessary. The Budapest Convention is the most feasible framework for new solutions.

Een fictieve situatie op een scherm tijdens de oprichting van het Defensie Cyber Commando. Defensie had al cybercapaci teiten voor defensieve taken en inlichtingen. Met het Defensie Cyber Commando wordt cyber volwaardig onderdeel van militaire operaties, inclusief de ontwikkeling van offensieve cybercapaciteiten.

A fictional situation on a screen during the launch of the Defence Cyber Command. The Netherlands Defence had already cyber capacity for defensive tasks and intelligence. With the Defence Cyber Command cyber becomes an integral part of military operations, including the development of offensive cyber capabilities.

ANP Valerie kuypers

By **Raymond Bierens**, external PhD candidate at Delft University of Technology and Chief Executive Officer at OBE-One

"Eén voor allen en allen voor één", schreef Alexandre Dumas in 1844. Cybersecurity is vandaag de dag eveneens één probleem voor allen. Maar werkt iedereen wel écht samen aan de oplossing voor dit ene probleem? De politieke wil lijkt er te zijn. Toch zijn er grote verschillen tussen de nationale en militaire cyberstrategieën van Amerika, Engeland, Duitsland en Nederland. Hoe komt dat? *"All for one and one for all", Alexandre Dumas wrote in 1844. In the present day, cyber security has become one problem for all. But is everyone really cooperating to find a solution for this one problem? There seems to be ample political will. Yet there are major differences in the national and military cyber strategies of the US, the UK, Germany and the Netherlands. How is this possible?*

NATIONAL CYBER STRATEGY REMAINS THE WORK OF PEOPLE

Raymond Bierens onderzoekt als buitenpromovendus aan de TU Delft naar mogelijke oorzaken van die verschillen. Terugkijkend zien we dat de eerste officiële nationale cyberstrategie in 2003 al door de Verenigde Staten werd gepubliceerd. In 2009 volgt Engeland. Nederland en Duitsland publiceren pas in 2011, hetzelfde jaar waarin Amerika z'n eerste strategie-update uitbrengt. Maar de verschillen tussen de landen gaan verder dan alleen de uitgiftedata. Scope, doel en budget van zowel de nationale als militaire cyberstrategieën verschillen eveneens aanzienlijk tussen deze vier landen.

Eerste onderzoeksresultaten

De eerste resultaten van het onderzoek tonen aan dat veel van de verschillen hun oorsprong vinden in de wijze waarop iedere overheid omgaat met het identificeren, interpreteren en managen van cyberrisico's. In dit proces kunnen drie achtereenvolgende fasen worden onderscheiden: 'risk identification', 'risk perception' en 'risk appetite'. Bij 'risk identification' worden risico's in kaart gebracht en vastgelegd in rapporten, zoals het jaarlijkse Cyber Security Beeld Nederland dat door het Nationaal Cyber Security Center in publiek-private samenwerking wordt uitgegeven. Een cyberrisico wordt pas zo aangemerkt als een combinatie van vertrouwde bronnen daartoe aanleiding geeft. Hierin hebben bijvoorbeeld de nationale inlichtingendiensten en Information Sharing and Analysis Centers (ISAC's) een rol.

Raymond Bierens, external PhD candidate at TU Delft, is investigating the possible causes for the enormous differences between the cyber strategies of these four countries. Looking back in time, we find that the first national cyber strategy was published by the United States as far back as 2003. The UK followed in 2009, and Germany and the Netherlands only published their strategies in 2011, the same year the US already presented its first strategy update. The publication date is but one of the differences between the countries. The scope, objectives and budgets of both the national and the military cyber strategies are significantly different between the four.

Preliminary results

The preliminary results of the study indicate that many of the differences stem from the different views the various governments have with respect to identifying, interpreting and managing cyber risks. Three subsequent phases can be identified in this process: risk identification, risk perception and risk appetite. Risk identification involves mapping the risks and detailing them in reports like the annual Cyber Security Assessment Netherlands published by the National Cyber Security Centre

Bij het bedrijf Fox-It waar het Defensie Cyber Commando wordt opgeleid. Dit is een groep van rond 13 militairen-hackers die getraind worden voor verdediging én aanval.
At the company Fox-It, where the Defence Cyber Command get trained. This is a group of around 13 soldiers-hackers who are trained for defense and attack.

Cyber Pearl Harbour

Het identificeren van cyberrisico's wordt vooral door experts gedaan. Daarna dienen besluitvormers overtuigd te worden van deze risico's en bijbehorende dreigingen. Experts spelen daar op in met metaforen als 'Cyber Pearl Harbour' (VS) of 'Deltaplan voor Cyber Security' (Nederland). Door de beeldvorming die daardoor ontstaat, neemt de politieke druk toe om de door de experts geïdentificeerde cyberrisico's te erkennen en aan te pakken. Dit proces en de weging die daaruit volgt, heet 'risk perception'.

Cover-your-ass

De erkenning van cyberrisico's door besluitvormers betekent nog niet dat ze ook daadwerkelijk aangepakt gaan worden. Dit hangt mede af van het beschikbare budget. Het komen tot een daadkrachtige aanpak wordt het proces van 'risk appetite' genoemd. Politieke overwegingen spelen hierin hoofdzakelijk een rol. Immers: geld uitgeven aan cybersecurity betekent dat het niet ergens anders naartoe kan gaan.

Lastige punten daarbij zijn dat cyberdreigingen nauwelijks zichtbaar zijn, de reële schade (nog) niet acuut genoeg is om dringende maatregelen te nemen en de economische schade pas op lange termijn voelbaar is. Het gevaar ligt daardoor op de loer dat geïdentificeerde risico's wel erkend worden, maar dat er onvoldoende budget beschikbaar wordt gesteld. Als gevolg daarvan wordt slechts beperkt actie ondernomen. Dit leidt tot een vals gevoel van veiligheid; experts noemen dit 'cover-your-ass cybersecurity'.

Eén voor allen en allen voor één. Dat is waar cybersecurity om vraagt. Het managen van cybersecurity-risico's over de landsgrenzen heen, kan echter alleen succesvol zijn als alle betrokkenen dezelfde prioriteiten stellen met respect voor elkaars nationale besluitvormingsprocessen.

---

in a public-private partnership. A cyber risk is only recognised as such when multiple reliable sources, like the national intelligence services and the Information Sharing and Analysis Centres (ISACs), indicate its existence.

Cyber Pearl Harbour

The identification of cyber risks is predominantly the job of experts. Once a risk has been identified, these experts are still to convince the decision-makers of the risk and the threat it poses. Phrases like 'Cyber Pearl Harbour' (US) and 'Delta Plan for Cyber Security' (Netherlands) are coined for this purpose. The picture painted by way of such wordings increases political pressure to recognise and tackle the risks identified by the experts. This process and the related weighting act is referred to as 'risk perception'.

Cover-your-ass

However, decision-makers recognising the existence of these cyber risks does not mean they will actually be tackled. The available budget plays an important part in this connection. Deciding on actually implementing an effective approach is referred to as the 'risk appetite' process. Political considerations play the main role in this regard, for allocating funds to cyber security means they cannot be used for something else. A real problem in this connection is that cyber threats are hardly visible, the concrete damage they cause is not (yet) so large they warrant taking urgent measures, and the economic damage caused will become noticeable only in the long term. As a consequence, while the identified risks may be recognised, insufficient funding may be provided to tackle them. The limited action taken with what little budget becomes available leads to a false sense of security, referred to by the experts as 'cover-your-ass security'.

All for one and one for all, that's what cyber security requires. But managing cyber security risks across national borders can only be successful if all those involved set the same priorities, with respect for each other's national decision-making processes.

By **Prof. B. Jacobs,** Radboud University, Nijmegen

Veel van de mechanische apparaten die we gebruiken vergen onderhoud, om de betrouwbaarheid te garanderen en de levensduur te verlengen. In veel landen wordt goed onderhoud van auto's zelfs afgedwongen, via periodieke verplichte keuringen. Hoe staat het met software, nu we daar steeds afhankelijker van worden, in het bijzonder via het zich ontvouwende Internet der Dingen? *Many of the mechanical appliances that we use require maintenance to ensure their reliability and extend their service life. Proper vehicle maintenance by way of periodic inspections is even compulsory in many countries. What is the score with software now that we are becoming more and more dependent on this, particularly via the developing Internet of Things?*

AFTERCARE FOR THE INTERNET OF THINGS

Software heeft ook onderhoud nodig, niet zozeer door slijtage, maar door het bekend raken van programmeerfouten of door veranderingen in de omgeving waarin de software gebruikt wordt. Er wordt dan gesproken van een software-update, of van een patch (wanneer het om herstel van fouten gaat). Het up-to-date houden van software kost geld. Fabrikanten doen dit om te voorkomen dat de gebruiker een softwarepakket van de concurrent installeert.

Geen zin in onderhoud

Het Internet der Dingen brengt met zich mee dat steeds meer apparaten in onze dagelijkse leefomgeving worden voorzien van een internetverbinding, variërend van tandenborstels tot kleding, en van thermostaten tot pacemakers. Deze apparaten kunnen daarmee op afstand uitgelezen en aangestuurd worden. Dit zou ons leven nog makkelijker moeten maken en externe partijen nog meer informatie moeten leveren over ons doen en laten, zodat ze hun prijzen en diensten nog gerichter kunnen afstemmen. Het Internet der Dingen draait op software die ingebed zit in apparaten. Als het apparaat eenmaal verkocht is, heeft de fabrikant zijn geld ontvangen, en is de motivatie beperkt om de software nog te onderhouden. Zeker wanneer de prijs laag is, zoals bij een lamp met een sensor die op afstand aangestuurd en uitgelezen kan worden. Worden we straks omringd door allerlei dingen met oude en kwetsbare software, waarbij de fabrikant geen zin meer heeft in onderhoud?

Zorgplicht

Als samenleving zullen we de ICT-sector zwaardere zorgplichten op moeten leggen. Wat niet werkt, is gedetailleerde eisen formuleren waar fabrikanten aan moeten voldoen. Bij een auto kun je redelijk precies beschrijven waar die aan moet voldoen. Maar een computer is een open apparaat dat voor vele doeleinden gebruikt kan worden. Belangrijker is het dus om fabrikanten te dwingen tot zorgzaamheid ten opzichte van

Software also requires maintenance, not so much due to wear but due to the recognition of programming errors or following changes to the environment in which the software is used. This is referred to as a software update or a patch (if this relates to the repair of errors). Keeping software up-to-date costs money. Manufacturers do this to ensure that users do not install competitor software packages.

The Internet of Things means that more and more appliances in our daily lives have an Internet connection from toothbrushes to clothes and thermostats to pacemakers. These appliances can therefore be read and controlled remotely. This should make our lives even easier and provide external parties with more information on what we do and don't do so they can set their prices and services even more accurately. The Internet of Things runs on software embedded into appliances. Once the appliance has been sold, the manufacturer has received its money and motivation is limited in still maintaining the software, certainly when the price is low as with a lamp with a sensor that can be controlled and read remotely. Will we soon be surrounded by all sorts of things with outdated and vulnerable software of which the manufacturer no longer has any interest in maintaining?

hun klanten. Van belang is om (1) vooraf fouten in software zoveel mogelijk te vermijden, en om (2) achteraf problemen zo snel mogelijk te herstellen en eventuele schade te vergoeden. Voor dat laatste moet de fabrikant (update)mechanismen hebben uitgewerkt, zeker voor producten die langere tijd mee gaan.

Onorthodox

Consumenten, industrie en overheden hebben een gezamenlijk (strategisch) belang bij uitgebreidere zorgplichten in de ICT. Mocht zulke klantenzorg uitblijven dan zijn mogelijk onorthodoxe maatregelen nodig. Te denken valt aan een wettelijke eis dat software die door de fabrikant niet meer wordt onderhouden automatisch open source wordt, zodat anderen het desnoods kunnen overnemen.
Overigens is het wel redelijk om generieke eisen te stellen aan fabrikanten, zeker als het gaat om het Internet der Dingen. Zo zouden er mogelijkheden moeten komen om historische gebruiksgegevens te wissen (bijvoorbeeld bij verkoop) of de verbinding met internet uit te schakelen als die niet essentieel is voor het functioneren van een apparaat.


Anoek Bleumer

Duty of care

We should as a society impose a stricter duty of care on the ICT sector. What is not working is formulating detailed requirements with which manufacturers must comply. With vehicles, you can describe reasonably accurately what is required of them. A computer is however an open appliance that can be used for many purposes. It is therefore more important to impose a duty of care on manufacturers with respect to their customers. What is important is (1) to avoid software errors as far as possible in advance and (2) to subsequently rectify problems as soon as possible and avoid any damage. The manufacturer should in the latter case have worked out (update) mechanisms, certainly for products lasting a long time.

Unorthodox

Consumers, industry and governments have a joint (strategic) interest in wider duties of care in ICT. Unorthodox measures may be necessary if such customer care is not forthcoming. An example could be a legal requirement for software that a manufacturer no longer maintains to become automatically open source so that others can take it over if necessary.

It is also reasonable to place generic requirements on manufacturers certainly as regards the Internet of Things. Possibilities should be introduced for deleting historical usage data (for example secondhand sale) or for disconnecting the Internet if this is not essential for the functioning of the appliance.

By **Prof. Dr. M.J.G. van Eeten**,
professor of Systems Engineering,
Delft University of Technology

Miljarden apparaten worden aan het internet gehangen zonder afdoende beveiliging. Fabrikanten besteden er te weinig aandacht aan en maken basale fouten. Daarom moet de goverance van het Internet der Dingen beter geregeld worden. *Billions of devices are plugged into the internet without adequate security. Manufacturers devote far too little attention to this problem and make fundamental errors. The governance of the Internet of Things needs to be better regulated.*

STRATEGIES FOR GOVERNANCE

De voorbeelden vliegen om de oren. Steeds vaker worden gebruiksvoorwerpen vanaf het internet gehackt., videorecorders, sluisbedieningen zelfs auto's. Twee onderzoekers namen via het internet een Jeep Cherokee over. Nadat deze kwetsbaarheid bekend werd, moest fabrikant Fiat Chrysler een officiële product recall doen. Hoe dede den ze dat? Ze stuurden alle eigenaren een USB-stick je via de post, met het verzoek die even in hun auto te stoppen om de firmware te updaten. Hebben we netiedereen uitgelegd dat zenietmeer lukraak USB-sticks in bedrijfscomputers moeten stoppen, krijgen mensen een stick je om in hun auto te stoppen. Het zou hilarisch zijn, als het niet ernstig voor woordenis. Want vergis je niet. In de wereld zijn inmiddels tientallen miljarden apparaten in omloop die aan het internet hangen: het Internet der Dingen. En de bulk is beroerd beveiligd.

Honeypot

Je kunt geen apparaat verzinnen of er is inmiddels een versie beschikbaar waarin een kleine computer zit met een complete protocolstack die graag met het internet praat. En waarvan de software ontstellend slecht is op het gebied van veiligheid. Samen met onderzoekers in Yokohama verzamelen we data met een zogenaamde 'Internet of Things Honeypot'. Oftewel, een lokdoos voor aanvallers van dit soort apparaten. We zien dat al tienduizenden systemen door hen

There is no shortage of examples. More and more consumer products and other items in daily use are being hacked through the internet, including refrigerators, video recorders, lock controls and even cars. Two researchers took control of a Cherokee Jeep through the internet. As soon as this vulnerability had been disclosed, Fiat Chrysler had to issue an official product recall. How did the hackers do it? They sent all the car owners a USB stick by post, instructing them to insert it in their car to update the firmware. Just when we had finished telling people not to insert USB sticks haphazardly into their computers, they did exactly that with a stick received by post! It would be hilarious if this was not such a deadly serious issue. Because worldwide, there are now billions of devices plugged into the internet: the Internet of Things. And the vast majority of those devices is very poorly protected.

Honey Pot

For almost every device you can think of, there is now a model on the market that contains a tiny computer with a complete protocol stack which is eager to start talking to the internet and has incredibly inadequate software in terms of security. In collaboration with researchers in Yokohama, we are collecting data using an 'Internet of Things Honey Pot' to attract the attackers of such devices. They have already taken control of tens of thousands of systems in video recorders, security camera's, routers, etc. The list is endless. What do they do with such control? To start with they use it to commit a range of 'standard' cyber crimes such as DDoS attacks. They are able to keep control of infected systems for long periods of time because many devices are difficult to clean up. In the 'usual' case of infected personal computers we have made a lot of progress in the past few

Mark Engelen

zijn overgenomen. Videorecorders, beveiligingscamera's, routers, ga maar door. Wat willen aanvallers ermee? In ieder geval gebruiken voor reguliere cybercrime zoals DDoS-aanvallen. Zij houden daarbij lang controle over de besmette systemen, omdat veel apparaten moeilijk op te schonen zijn. Bij 'gewone' besmette personal computers hebben we behoorlijke vooruitgang geboekt de afgelopen jaren. Softwarefabrikanten, internetaanbieders en antivirusbedrijven zijn beter geworden in het voorkomen en opruimen van besmettingen. Maar wie gaat straks mijn videorecorder of zonnepaneel ontsmetten? Gaan we daar antivirus opzetten?

Governance

Dat brengt ons bij de kern van het probleem: governance. Hoe krijgen we dit ooit in de greep? Er zijn een paar strategieën denkbaar.

1. Bewustwording: bedrijven en consumenten

years. Software producers, internet providers and virus protection companies are now much better at preventing and cleaning up PC infections. But who is going to remove the virus from my video recorder or solar panel? Should we install antiviral software in these devices as well?

Governance

This brings us to the core of the problem: governance. Can we achieve effective governance, and if so how? There are a number of possible strategies.

1. Raising awareness: businesses and consumers should think twice, weigh up the risks and

HET INTERNET DER DINGEN IS BEROERD BEVEILIGD

THE INTERNET OF THINGS IS POORLY PROTECTED

die apparaten aan internet hangen moeten daarover nadenken, risico's afwegen en kiezen wat zij wel en niet aan zo'n apparaat toestaan.

2. Transparantie: laten we in ieder geval inzichtelijk maken wat voor apparaten we geleverd krijgen, welke internetfunctionaliteit er aan hangt en wat met de verzamelde data wordt gedaan.
3. Monitoring: het volgen van wat er mis gaat kan beter. Dat is een stimulans voor bedrijven om transparant te zijn.
4. Standaarden en keurmerken: We hebben KEMA voor elektriciteit, waarom dan niet zoiets voor cybersecurity?
5. Aansprakelijkheid: schade en het 'opruimen' van digitale rommel moeten voor rekening van fabrikant of leverancier komen.
6. Versterken van gebruikersrechten en privacy: we stellen grenzen aan al te gretige datahonger om daarmee bepaalde risico's in te dammen.
7. Intermediaire verantwoordelijkheid: bedrijven en organisaties die een rol kunnen vervullen in de cybersecurity van het Internet der Dingen krijgen daarin verantwoordelijkheid. Denk aan internetaanbieders die botnets blokkeren. Zij moeten dan ook maar mijn videorecorder of zonnepaneel blokkeren als die meedoen aan een DDOS-aanval.

Geen van deze antwoorden is op zichzelf afdoende. Vermoedelijk hebben we ze allemaal nodig. Liefst morgen. Of in ieder geval voordat die apparaten op dezelfde schaal gehackt worden als onze pc's. Dat moment is niet ver weg.

---

make clear choices about what is permissible before plugging their devices into the internet.

2. Transparency: we should in any case have a clear understanding of the devices supplied to us and the internet functionality they are plugged into. We should also know exactly what happens to the data collected by our devices.
3. Monitoring: there is plenty of room for improvement when it comes to keeping track of what is happening, especially when things go wrong. This is an incentive for businesses to be transparent.
4. Standards and quality labels: We already have a KEMA (Testing, Research and Engineering Consultants to the Electric Power Industry).Why not something similar for cyber security?
5. Liability: the manufacturer or supplier should be held liable for damages and the 'clean-up' of digital junk.
6. Reinforcing user rights and privacy: we should place limits on the seemingly endless hunger for data to contain certain risks.
7. Intermediary responsibility: companies and organisations that could contribute to the cyber security of the Internet of Things should be given responsibility for doing so. Internet providers for example can block 'botnets'. They should also be obliged to block my video recorder, or my solar panel, if they starting taking part in a DDOS attack.

None of these strategies is sufficient on its own. We probably need all of them. Preferably at the earliest opportunity. Or at least before such devices are hacked on the same scale as our PCs. That moment may not be far away.

CYBER SECURITY COUNCIL HIGHLIGHTS 2014-2016

De Cyber Security Raad is van mening dat cybersecurity de verantwoordelijkheid is van de boardroom. De CSR heeft een handreiking voor bestuurders opgesteld, die hen helpt strategisch niveau sturing te geven aan cybersecurity en het onderwerp strategisch in de organisatie te beleggen. Bedrijven moeten structureel bouwen aan digitale veiligheid . De CSR leden houden daarom ieder jaar een aantal boardroomgesprekken met de board van bedrijven uit de Nederlandse vitale sector. Op informele wijze wisselen raadsleden kennis en ervaring uit, om de board te ondersteunen bij hun cybersecurity aanpak.

Advies cybersecurity in onderwijs en bedrijfsleven

Een belangrijk moment voor de CSR is het uitbrengen van het advies cybersecurity in onderwijs en bedrijfsleven aan de staats secretarissen van Onderwijs en Veiligheid en Justitie geweest. Het advies is opgesteld in samenwerking met diverse partijen en goed ontvangen door de betrokken partijen en stakeholders. De kern van het advies is dat een goede en structurele voorbereiding van de jeugd op de digitale toekomst van groot belang is. Niet alleen omdat scholieren van nu, de workforce van morgen zijn maar ook omdat de economische welvaart van een land mede afhangt van de juiste kennis van de bevolking. Het feit dat we afstevenen op een tekort aan cybersecurityspecialisten in de nabije toekomst is zorgelijk. Onderwijs en bedrijfsleven moeten de handen ineen slaan om nu en in de toekomst voldoende specialisten af te leveren. Daar blijft de CSR zich voor inzetten.

Internet der Dingen (IoT)

Het onderwerp voor de komende jaren waarover de CSR zich zal buigen is IoT. Het feit dat alles met alles verbonden wordt en groten deels al is, apparaten die met elkaar praten en ontelbare hoeveelheden (privacy) gevoelige data verspreiden, is een groot issue de komende jaren. Veel mensen zijn zich nog niet bewust van de grote ommekeer die het IoT zal brengen. We staan midden in het digitale tijdperk. De Cyber Security Raad zal zich buigen over te nemen maatregelen om het Internet der Dingen op verantwoorde wijze te laten landen in de samenleving.

Zorgplichten

De Raad ziet tevens het belang in van een juiste invulling van de zorgplicht door bedrijven en organisaties. Wat voor rollen en verantwoordelijkheden komen er voort uit de diverse wet en regelgeving op het gebied van de zorgplichten? Wie is waarvoor verantwoordelijk? Waar kan een burger naar toe als hij /zij het slachtoffer is van cybercrime, privacy issues of aansprakelijkheids issues? Bestaande en nieuwe wet en regelgeving zijn op dat vlak niet altijd eenvoudig en eendui dig toepasbaar voor organisaties. De Raad zal daarom op basis van een juridisch kader een handreiking zorgplichten opstellen.

The Cyber Security Council feels that cyber security is a boardroom responsibility. The CSR has drawn up a practical guide for boardroom members, which helps them to provide cyber security guidance on a strategic level and to strategically embed the subject in the organisation. Businesses have to pay attention to digital security structurally. It is for this reason that CSR members conduct a number of boardroom discussions every year with the boards of companies in key sectors of the Netherlands. Council members exchange knowledge and experiences in an informal manner to assist the board in its cyber security approach.

Cyber Security recommendation in education and the business community

An important occasion for the CSR was to provide the recommendation cyber security in education and the business community to the State Secretaries of Education and Security and Justice. The recommendation was drawn up in conjunction with various parties, and was well received by the parties and stakeholders involved. The essence of the recommendation is that a sound and structural preparation of the youth for the digital future is of vital importance. Not only because the students of today will be the workforce of tomorrow, but also because the economic welfare of a country depends on the population having the right knowledge. The fact that we re heading for a shortage of cyber security specialists in the near future, is troublesome. The education sector and the business community must join forces to be able to deliver enough specialists now and in the future. The CSR continues to be committed to this.

Internet of Things (IoT)

The topic which the CSR will concentrate on in the forthcoming years is IoT. The fact that everything will be connected with everything and largely already is, devices that communicate with each other and distribute innumerable quantities of (privacy)sensitive data, is a major issue in the coming years. Many people are not yet aware of the massive transformation that IoT will bring about. We re standing right in the middle of the digital era. The Cyber Security Council will deliberate on taking measures to embed the Internet of Things in society in a responsible manner.

Duty of due care

The Council also sees the importance of a correct interpretation of the duty of due care by businesses and organisations. What roles and responsibilities will arise from the various legislation and regulations in the field of duty of due care? Who is responsible for what? Where can citizens go when they are victim to cyber crime, have privacy issues or have liability issues? On that level existing and new legislation and regulations are not always easily and unambiguously applicable for organisations. So, on the basis of a legal framework, the Council will draw up a practical guide on duty of due care .

Colofon ◦ *Colophon*

Opdrachtgever ***Commissioning party***: Cyber Security Raad Nederland, *Dutch Cyber Security Council*
Hoofdredactie ***Chief editor***: Elly van den Heuvel
Redactie ***Editors***: Eline Attema, Danja Zwijnenburg en Martin Bobeldijk (Turnaround Communicatie)
Vertalingen ***Translations***: Concorde
Concept en processupervisie ***Draft and process supervision***: Eline Attema, Danja Zwijnenburg en Martin Bobeldijk (Turnaround Communicatie)
Grafische vormgeving ***Graphic design***: Tappan Communicatie
Drukwerk ***Printing***: De Bink

CSR Cyber Security Council Cyber Security Raad