CSR MAGAZINE

Cyber Security Council
Cyber Security Raad

Gouden driehoek helpt cybersecurity vooruit ◦ Digitale domein beperking én kans voor de nationale economie ◦ Cybersecurity hoort thuis in elke boardroom ◦ Meer internetveiligheid begint bij beter onderwijs ◦ Responsible disclosure and repair ◦ Strafrecht is niet zaligmakend Golden triangle helps progression of cyber security ◦ Cyber security: limitation and opportunity ◦ Cyber security belongs in the boardroom ◦ Greater internet security starts with better education ◦ Responsible disclosure and repair ◦ Criminal law is not the universal remedy

Year 1, No 1, april 2015

PUBLIEK-PRIVATE PARTICIPATIE

PUBLIC-PRIVATE PARTICIPATION

Nederland behoort tot de top van Europa, en in sommige opzichten zelfs van de wereld, als het gaat om het gebruik van ICT-toepassingen. Dat stimuleert maatschappelijke en economische groei, maar maakt ook kwetsbaar.

Cybercriminelen – statelijk of niet statelijk – gebruiken geavanceerde methoden om in ons land delicten te plegen. De laatste jaren zien we dat een effectieve aanpak alleen mogelijk is als publieke, private en wetenschappelijke partners participeren in een effectief samenwerkingsverband. Deze 'gouden driehoek' of 'triple helix' vormt de basis van de Cyber Security Raad (CSR). De combinatie én confrontatie van deze verschillende disciplines en belangen leiden tot belangrijke en vernieuwende strategische inzichten.

De afgelopen vier jaar heeft de Raad een bijdrage geleverd aan de nationale cybersecurity-strategie. Veiligheid, vrijheid en economische ontwikkeling staan daarin centraal. Ook heeft de Raad diverse keren het kabinet van advies voorzien en is een aantal belangwekkende onderzoeken opgestart. De leden spannen zich individueel in voor een digitaal veilig Nederland door boardroomgesprekken te voeren bij bedrijven met vitale processen voor ons land. Deze gesprekken hebben tot doel cybersecurity hoger op de agenda te krijgen. Ook de komende jaren zal de CSR zich buigen over complexe strategische vraagstukken en de internationale positie versterken door samenwerking te zoeken met vergelijkbare raden in andere landen.

Het is ons een genoegen om dit magazine bij u te introduceren, zodat u de CSR en zijn werkzaamheden leert kennen. Het is onze wens dat we gezamenlijk (inter)nationaal in staat zullen zijn de handen ineen te slaan voor een open, vrij en veilig internet.

Namens de Cyber Security Raad,
Drs. E. Blok, co-voorzitter Cyber Security Raad
Drs. H.W.M. Schoof, co-voorzitter Cyber Security Raad

The Netherlands belongs to the European top, and in some ways to the world top, when it comes to the use of ICT applications. It stimulates societal and economic growth, but also creates weaknesses.

Cyber criminals, whether they are state actors or not, use advanced methods to commit cyber crimes in our country. Over the last few years, we have seen that an effective approach is only possible if public, private and scientific partners participate in an effective partnership. This 'golden triangle' or 'triple helix' forms the basis of the Cyber Security Council (CSR). The combination and confrontation of these different disciplines and interests have led to important and innovative strategic insights.

In the past four years, the Council has made contributions to the national cyber security strategy. Security, freedom and economic development are the central issues. The Council has also advised the cabinet on numerous occasions and initiated several major research programs. Its members individually work towards achieving a digitally safe country by conducting board room meetings at companies in the vital sector. The ultimate goal of these meetings is to garner more attention for cyber security. In the medium to long term, the CSR will also explore complex strategic issues and strengthen its international position by seeking partnerships with similar Councils on other countries.

The CSR is a strategic advisory council to the cabinet. We are very pleased to introduce you to this magazine, which is intended to acquaint you with the CSR and its work. It is our wish that we will be able to establish joint partnerships, nationally and internationally in order to achieve an open, free and safe internet.

On behalf of the Cyber Security Council,
Drs. E. Blok, co-chairman Cyber Security Council
Drs. H.W.M. Schoof, co-chairman Cyber Security Council

INHOUD CONTENTS

CSR Cyber Security Council | Cyber Security Raad

De Cyber Security Raad ◦ The Cyber Security Council

Van links naar rechts ◦ *From left to right*: **Bas Eenhoorn, Eelco Blok** (co-voorzitter ◦ *co-chairman*), **Gerrit van den Burg, Dick Heerschop, Elly van den Heuvel** (secretaris ◦ *secretary*), **Rob Bertholee, Rob Bauer, Pieter Schoehuijs, Michel van Eeten, Bart Hogendoorn, Ben Voorhorst, Arjen Dorland, Tineke Netelenbos, Dick Schoof** (co-voorzitter ◦ *co-chairman*), **Wilma van Dijk, Bart Jacobs**
Niet op deze foto ◦ *Not on this picture*: **Mark Dierikx**
Photo: Mark Janssen

De Cyber Security Raad adviseert het kabinet over het vergroten van de cybersecurity in Nederland. In de Raad werken drie partijen nauw samen: de overheid, het bedrijfsleven en de wetenschap. Hoe is het gesteld met de cybersecurity in Nederland? En hoe brengen de drie partijen hun belangen op één lijn? Dick Schoof, Eelco Blok en Michel van Eeten geven hun visie en vertellen over hun ervaringen in de Raad. *The Cyber Security Council advises the cabinet on expanding cyber security in the Netherlands. There's close collaboration between three parties in the Council: the government, the business community and the academic community. What is the state of cyber security in the Netherlands? And how do the three parties coordinate their interests? Dick Schoof, Eelco Blok and Michel van Eeten give their opinion and tell about their experiences in the Council.*

GOUDEN DRIEHOEK HELPT CYBERSECURITY IN NEDERLAND VOORUIT

GOLDEN TRIANGLE HELPS PROGRESSION OF CYBER SECURITY IN THE NETHERLANDS

Aan tafel zitten drie mensen: Nationaal Coördinator Terrorismebestrijding en Veiligheid Dick Schoof, bestuursvoorzitter KPN Eelco Blok en hoogleraar Bestuurskunde bij de Technische Universiteit Delft Michel van Eeten. Samen met twaalf andere topmensen uit het bedrijfsleven, de wetenschap en de overheid vormen zij de Nederlandse Cyber Security Raad. Schoof en Blok zijn samen voorzitter van de Raad.

Schoof steekt direct van wal: ´Hoe motiveren we bedrijven en organisaties om cybersecurity hoog op de agenda te zetten? Hoe zorgen we ervoor dat universiteiten en hogescholen voldoende gekwalificeerde mensen opleiden? Hoe kunnen we het basis- en het voorgezet onderwijs meenemen in de digitale wereld? Hoe spelen we tijdig en effectief in op nieuwe technologische ontwikkelingen? Op deze vragen proberen we gezamenlijk een goed antwoord te vinden in de Cyber Security Raad. Cybersecurity is niet alleen een technisch vraagstuk, maar ook een gedrags- en kennisvraagstuk.'

De impact van cyber

Cybersecurity is voor het Nederlandse bedrijfsleven van groot belang, vertelt Blok. Blok zit in de Raad namens werkgeversorganisatie VNO-NCW. 'Cybercrime is een reële bedreiging voor de continuïteit van bedrijven. Als je je realiseert wat de impact kan zijn van

The three people at the table are: The National Coordinator for Counterterrorism and Safety Mr. Dick Schoof, the Chairman of the Board of KPN Mr. Eelco Blok and Professor of Public Administration at the University of Technology Delft Mr. Michel Van Eeten. Together with twelve other leaders from the business and academic community and the government, they form the Dutch Cyber Security Council. Schoof and Blok together, are chairman of the Council.

Schoof immediately kicks off: ´How do we motivate companies and organisations to place cyber security high on the agenda? How do we ensure that universities and colleges educate sufficiently qualified people? How can we incorporate primary and secondary education in the digital world? How do we effectively and timeously anticipate new technological developments? These are the issues which we jointly seek to resolve in the Cyber Security Council. Cyber security is not only a technical issue, but also concerns behavioural and knowledge problems.'

The impact of cyber

Cyber security is of paramount importance for the Dutch business community, says Blok. Blok is a member of the council on behalf of the employers' organisation VNO-NCW. 'Cybercrime is a genuine threat for the continuity of businesses. When you realise what the impact of cyber attacks could be, then it's logical that VNO-NCW

‘DE BELANGEN LOPEN NIET ALTIJD PARALLEL, MAAR WE HEBBEN GEEN VERSCHIL VAN MENING OVER ONS EINDDOEL: DE WEERBAARHEID VAN NEDERLAND VERGROTEN.’ Eelco Blok

‘THE INTERESTS DON’T ALWAYS RUN PARALLEL, BUT WE DON’T DIFFER IN OUR OPINIONS ABOUT OUR ULTIMATE GOAL: INCREASING THE RESILIENCE OF THE NETHERLANDS.’ Eelco Blok

‘CYBER VORMT EEN BELANGRIJKE MOTOR VOOR ONZE ECONOMIE, DAAR PROFITEREN WE ALLEMAAL VAN.’ Dick Schoof

‘CYBER FORMS A SIGNIFICANT ENGINE FOR OUR ECONOMY, WE ALL BENEFIT FROM IT.’ Dick Schoof

cyberaanvallen, dan is het logisch dat VNO-NCW een bijdrage levert aan de Cyber Security Raad. Met elkaar proberen we de weerbaarheid van Nederland te versterken.’

Wetenschapper Van Eeten benadert cybersecurity vooral vanuit een economisch perspectief. Wat zijn de incentives voor marktspelers om wel of niet iets aan cybersecurity te doen? Elk bedrijf maakt daarin keuzes. Van Eeten: ‘Kosten en baten raken al snel uit balans bij cybersecurity. Standaardreflex van security-experts is alle vormen van onveiligheid terug te dringen, maar dat is onzin. Vergelijk het met winkeldiefstal: dat kun je ook niet voor honderd procent voorkomen. Dan zou winkelen duur en onplezierig worden. Dan is het soms beter je klanten te compenseren bij cyberschade, zodat ze zonder zorgen je product kunnen gebruiken.’

Samen meters maken

De samenwerking tussen de drie partijen in de Cyber Security Raad is internationaal gezien uniek, vertelt Schoof. ‘Het past goed bij de Nederlandse cultuur, waarin we van oudsher zijn gericht op consensus. Omdat alle belangrijke partijen aan tafel zitten, kunnen we echt meters maken. Daarom noemen we de samenwerking tussen deze drie partijen ook wel de gouden driehoek.’

Maar is de samenwerking tussen de drie partijen soms niet lastig? De belangen kunnen ook uiteen lopen. Blok knikt: ‘Natuurlijk, onze belangen lopen niet altijd parallel. Maar ik heb de afgelopen jaren gemerkt dat we geen verschil van mening hebben over ons einddoel: de weerbaarheid van Nederland vergroten op het gebied van cybersecurity. Dat is wat deze Raad zo krachtig maakt. We hebben goeddeels dezelfde ideeën over wat daarvoor moet gebeuren. Alleen verschillen we soms over de manier waarop je dat bereikt. Daarom is het goed om aan één tafel te zitten om verschillen van inzicht te bespreken en om te kijken of je naar elkaar toe kunt komen. Dat is tot nu toe altijd gelukt.’

Je mening bijstellen

Van Eeten vindt dat de waarde van de Raad vooral in het gesprek zit. ‘De raadsleden zitten op een belangrijke strategische plek, ze krijgen van elkaar nieuwe informatie en beïnvloeden elkaar. Ik weet zeker dat elk raadslid zijn mening wel eens heeft bijgesteld door een discussie in de Raad. Dat geldt ook voor mij en dat is heel

provides a contribution to the Cyber Security Council. Together we try to enhance the safety and resilience of the Netherlands.’

The scientist Van Eeten approaches cyber security mainly from an economics perspective. What are the incentives for market parties to do something, if anything, about cyber security? Every business makes such choices. Van Eeten: ‘Costs and benefits easily get unbalanced with cyber security. The standard reflex of security experts is to reduce all forms of insecurity, but that is nonsense. Compare it to shoplifting: you cannot prevent that entirely. Then shopping would become expensive and unpleasant. Sometimes it’s better to compensate your clients for cyber damage so that they’re able to use your product without worries.’

Making progress together

In international terms, the collaboration between the three parties in the Cyber Security Council is considered to be unique, says Schoof. ‘It suits the Dutch culture very well, in which and by tradition we’re always striving for consensus. It’s because all the important parties are present that we’re able to make progress. That’s why we tend to call the collaboration between these three parties the golden triangle.’

But isn’t the collaboration between the three parties sometimes difficult? The interests could also differ. Blok nods: ‘Naturally, our interests don’t always run parallel. But in recent years I’ve noticed that we don’t have a difference of opinion about our ultimate goal: increasing the safety and resilience of the Netherlands in the field of cyber security. That is what makes this council so powerful. For the most part we have the same ideas about what should happen to achieve this. We only differ sometimes about the manner in which that is achieved. That’s why it’s good for all of us to sit at one table to discuss differences of

‘DE CSR VOLGT NIET KLAKKELOOS DE ONTWIKKELINGEN, MAAR WIL DE TERREINEN ONTDEKKEN WAAR MEER RICHTING NODIG IS.’ Michel Van Eeten

THE CSR DOESN’T JUST SIMPLY MONITOR THE DEVELOPMENTS UNQUESTIONINGLY, BUT WANTS TO DISCOVER THE GROUNDS THAT NEED MORE DIRECTION.’ Michel Van Eeten

waardevol. Wat ik verder goed vind, is dat de Raad steeds meer gaat nadenken over welk gesprek in Nederland nog te weinig wordt gevoerd. We volgen niet klakkeloos de ontwikkelingen, maar willen de terreinen ontdekken waar meer richting nodig is. In die zin lopen we vooruit op de beleidscyclus. Wij praten nú over de onderwerpen die over twee jaar naar de Tweede Kamer gaan.’

In Nederland wordt ook op operationeel niveau door de drie partijen samengewerkt. Blok heeft daarbij veel waardering voor de rol van het Nationaal Cyber Security Centrum (NCSC): ‘Het is een overheidsorganisatie waar veel kennis en kunde is gebundeld. Als er incidenten zijn of waarschuwingen uit het buitenland komen, dan is het NCSC de spin in het web. Het centrum speelt informatie door en adviseert over de juiste maatregelen. Het NCSC is van groot belang voor ons land en wordt door het bedrijfsleven erg gewaardeerd.’

‘CYBERCRIME IS EEN REËLE BEDREIGING VOOR DE CONTINUÏTEIT VAN BEDRIJVEN.’ Eelco Blok

‘CYBERCRIME IS A GENUINE THREAT FOR THE CONTINUITY OF BUSINESSES.’ Eelco Blok

Van betekenis zijn

Dat is mooi, maar wat levert die samenwerking Nederland eigenlijk op? Wat wordt de burger er beter van? Schoof: ´Het cyberdomein is nauw verweven met ons dagelijkse leven. Drie aspecten zijn daarbij van groot belang: economie, veiligheid en privacy. Ze houden elkaar in evenwicht, maar ze bewegen wel. Cyber vormt een belangrijke motor voor onze economie, daar profiteren we allemaal van. Maar burgers willen het digitale domein alleen gebruiken als het veilig is. Zo bezien is veiligheid een economisch principe. Ook het aspect van privacy is belangrijk: consumenten moeten zich vrij kunnen bewegen op het internet in de wetenschap dat hun informatie alleen komt op de plekken waarvoor het is bedoeld. Als we dat met elkaar kunnen bereiken, dan is de Raad van betekenis.’

opinion and to see whether we can come to some sort of agreement. Up to now that’s always been the case.’

Adjusting your opinion

Van Eeten thinks that the council’s true value, above all, is the discussions themselves. ‘The Council members hold prominent strategic positions, they get new information from each other and influence each other. I’m sure that every councillor has adjusted his/her opinion at some point because of a discussion in the Council. That applies to me too and that’s extremely valuable. What I further consider to be a good thing, is that the council is thinking more and more about which debates are not being held often enough in the Netherlands. We don’t just simply monitor the developments unquestioningly, but want to discover the grounds that need more direction. In that sense we’re ahead of the policy cycle. Right now we’re discussing topics which will be sent to the Lower House in two years’ time.’

The three parties also collaborate in the Netherlands on an operational level. Here Blok expresses much appreciation for the part played by the National Cyber Security Centre (NCSC): ‘It’s a government organisation where a great deal of knowledge and expertise is clustered. When there are incidents or warnings from abroad then the NCSC acts as the spider in the web. The centre passes on information and gives advice on the right actions. The NCSC is of vital importance to our country and is highly appreciated by the business community.’

Being important

That’s all good and well, but what are the benefits of this collaboration for the Netherlands? Are the citizens better off? Schoof: ´The cyber domain is closely interwoven with our daily lives. In this, three aspects are of vital importance, being the: economy, security and privacy. They keep each other in a mutual balance, but they do shift. Cyber forms a significant engine for our economy, we all benefit from it. But citizens only want to use the digital domain if it is secure. Looking at it from that perspective, security is an economic principle. The privacy aspect is also important: consumers must be able to move freely over the internet knowing that their information only ends up at the places where it’s meant to be. If we can achieve that together, then the Council has meaning.’

Hoe werkt de Cyber Security Raad in Nederland?

- De Cyber Security Raad (CSR) werd opgericht in 2011.
- De CSR bestaat uit vijftien raadsleden die werkzaam zijn op strategische plekken in het bedrijfsleven, in de wetenschap en bij de overheid. Eind 2015 groeit de raad naar achttien leden: zeven vanuit de overheid, zeven van het bedrijfsleven en vier vanuit de wetenschap.
- De CSR volgt de uitvoering van de Nationale Cybersecurity Strategie 2 en geeft gevraagd en ongevraagd adviezen aan het kabinet.
- De raadsleden van de CSR voeren boardroomgesprekken om bestuurders van grote bedrijven en organisaties bewuster te maken van het belang van cybersecurity.
- De CSR stelt werkgroepen in rond de thema's uit het jaarlijkse Werkplan. In 2014 waren er werkgroepen over onder andere zorgplicht, standaarden en onderwijs en arbeidsmarkt.
- De Bureausecretaris ondersteunt de CSR bij het behalen van de resultaten.

How does the Cyber Security Council in the Netherlands operate?

- The Cyber Security Council (CSR) was established in 2011.
- The CSR comprises fifteen council members who work in strategic positions in the business community, in the academic community and in the government. At the end of 2015 the council will increase to eighteen members: seven from the government, seven from the business community and four from the academic community.
- The CSR monitors the execution of the National Cyber Security Strategy 2 and offers solicited and unsolicited advice to the cabinet.
- The council members of the CSR conduct boardroom meetings to make managers of major companies and organisations more aware of the importance of cyber security.
- The CSR appoints working groups for the themes included in the annual Working Plan. In 2014 there were working groups which included an obligation to care, standards and education, and the labour market.
- The office of the secretary supports the CSR in achieving the results.

Slimme meters en e-health

De afgelopen jaren heeft de Cyber Security Raad tal van adviezen gegeven die navolging kregen. Het beleid rondom responsible disclosure is hier een mooi voorbeeld van. De komende jaren wordt de 'Internet of Things' een enorme uitdaging. Steeds meer apparaten in en om het huis worden digitaal aangestuurd, denk aan slimme energiemeters en aan e-health. Hoe meer apparaten met het internet zijn verbonden, hoe groter het risico op incidenten. Er komen in onze huizen dus steeds meer digitale toegangspunten die een potentieel risico vormen vanuit cybersecurity.
Van Eeten knikt: 'Het lastige van de 'Internet of Things' is bovendien dat het zo gefragmenteerd is. Het gaat om veel verschillende apparaten, veel leveranciers en allerlei nieuwe software die niet altijd van goede kwaliteit zal zijn. Hoe krijgen we dit op orde? Zorgplicht invoeren wordt heel lastig. Want wie moet ervoor zorgen dat we deze producten veilig kunnen gebruiken? De winkel waar je het apparaat koopt, de importeur of de producent van het apparaat?'

Vitale infrastructuur

'Daarnaast vind ik het belangrijk dat we meer zicht krijgen op de cybersecurity in onze vitale infrastructuur', vervolgt Van Eeten. 'Bijvoorbeeld bij de waterbedrijven, in de ziekenhuizen en de telecomsector. Hoe zorgen we ervoor dat zij voldoende investeren én dat zij in de juiste zaken investeren? Dat kunnen we niet helemaal aan zelfregulering overlaten, vind ik.'

Blok vult aan: 'Veel bedrijven in de vitale infrastructuur hebben de afgelopen jaren goede stappen gezet. Zo hebben de telecom- en energiesector oefeningen uitgevoerd op het gebied van cybersecurity. Met deze oefeningen hebben ze beter zicht gekregen op de plekken waar ze hun weerbaarheid kunnen versterken in geval van een cyberincident.'
De Cyber Security Raad steunt dit soort initiatieven, want het uitwisselen van de resultaten zorgt ervoor dat andere sectoren geïnspireerd raken. Dat is belangrijk, want veel sectoren zijn van elkaar afhankelijk. Blok: 'We moeten dus werken aan een standaardaanpak van cyberincidenten over de sectoren heen. Dat wordt een belangrijke uitdaging voor de komende jaren.'

Transparantie organiseren

Van Eeten ziet nog een andere uitdaging: 'We kunnen een hoop problemen oplossen door transparantie bij bedrijven te organiseren. Het zou mooi zijn als we weten welke bedrijven goed presteren op het gebied van digitale veiligheid en welke niet. Dat ontbreekt nu nog. Welke provider of betaaldienst moet je kiezen als je veiligheid belangrijk vindt? Als consumenten daar beter zicht op hebben, gaat dat zeker markteffecten hebben. Dan gaan meer bedrijven investeren in cybersecurity zonder dat we ze dwingende normen of certificering opleggen. Want we weten dat dergelijke ingrepen duur zijn en maar weinig veiligheid opleveren.'

Schoof vindt dat het cybersecurity-stelsel in Nederland goed is geregeld. Er is een meerjarenstrategie, een goed functionerend cybercentrum én een strategische raad. 'De cybersecurity in Nederland is internationaal gezien van hoog niveau', vertelt Schoof. 'Maar het succes van vandaag is de nederlaag van morgen. We moeten ook kleinere organisaties in ons land meenemen in de ontwikkeling van cybersecurity. Bedrijven die de afgelopen jaren geen aandacht hebben besteed aan cybersecurity zijn verder achterop geraakt. Kortom, we moeten blijven investeren.'

Flinke sprong voorwaarts

De Global Conference on Cyberspace 2015 is daarbij belangrijk voor Nederland. 'We gaan als land er alles aan doen om ervoor te zorgen dat de conferentie een succes wordt', vertelt Schoof. 'We willen graag nieuwe internationale afspraken maken, zodat we met elkaar het niveau van cybersecurity verder kunnen verhogen. Daarnaast is Nederland voorzitter van de Europese Unie in de eerste helft van 2016. Cybersecurity is één van de topprioriteiten tijdens dat voorzitterschap. In Europa is nog veel te winnen op dit punt. We hopen een flinke sprong voorwaarts te maken. Zowel met het vergroten van cybersecurity als het terugdringen van de cybercrime in Europa. De Cyber Security Raad levert daar ook een waardevolle bijdrage aan.'

'CYBERSECURITY HOORT THUIS IN DE BOARDROOM. HET IS EEN STRATEGISCH VRAAGSTUK DAT ZELFS DE NATIONALE VEILIGHEID KAN RAKEN.' Dick Schoof

'CYBER SECURITY BELONGS IN THE BOARDROOM. IT IS A STRATEGIC ISSUE THAT CAN EVEN AFFECT NATIONAL SECURITY.' Dick Schoof

Smart meters and eHealth

In recent years the Cyber Security Council has provided many recommendations which were followed through. The policy concerning responsible disclosure is a fine example of this. In the forthcoming years the 'Internet of Things' will become an enormous challenge. More and more devices in and around the home are controlled digitally. For example, smart energy meters and eHealth. The more devices connected to the internet, the greater the risk of incidents occurring. Our homes are gradually getting more online access points which are a potential risk from a cyber security point of view.

Van Eeten nods in agreement: 'Besides, the difficulty with the 'Internet of Things' is that it is so fragmented. It concerns many different devices, multiple suppliers and all kinds of new software which will not always be of good quality. How are we going to organise this? It'll be difficult to introduce an obligation of caring. Because, who has to ensure that these products can be used safely? The shop where the device was bought, the importer or the manufacturer of the device?'

Critical infrastructure

'In addition I think it's important that we shed more light on the cyber security of our critical infrastructure', Van Eeten continues. 'For instance at the water companies, in the hospitals and in the telecoms sector. How do we ensure that they invest enough as well as invest in the right businesses? I don't think we could leave that entirely up to self-regulation.'

Blok adds: 'Many businesses in critical infrastructure have taken positive steps in recent years. The telecom and energy sectors have carried out exercises in the field of cyber security. These exercises have provided them with a better insight into the places where they can enhance their resilience in case of a cyber incident.'
The Cyber Security Council supports these types of initiatives, because exchanging results could ensure that other sectors become inspired. That is important, because many sectors are dependent on one another. Blok: 'We therefore have to work on a standard approach of cyber incidents across all the sectors. That will be a significant challenge in the forthcoming years.'

Organising transparency

Van Eeten sees another challenge: 'We can resolve many issues by organising transparency at businesses. It would be nice to know which businesses perform well in the field of cyber security and which don't. That's what's still missing. Which provider or payment service must you choose if you think security is important? If consumers were informed better about that, it would certainly have an effect on the market. Then more businesses will invest in cyber security without us having to impose mandatory standards or certifications. We know that such interventions are expensive and only bring about a limited amount of security.'

Schoof thinks that the cyber security system in the Netherlands is well organised. There's a multi-annual strategy, a well functioning cyber centre as well as a strategic council. 'On an international level the cyber security in the Netherlands is of a high calibre', says Schoof. 'But the success of today is the downfall of tomorrow. We must also include smaller organisations in our country in the development of cyber security. Businesses which have not paid any attention to cyber security in recent years are lagging behind even further. In short, we must continue to invest.'

Considerable stride forwards

The Global Conference Cyberspace 2015 is important for the Netherlands. 'As a country we will do everything in our power to ensure that the conference is successful', says Schoof. 'We would like to make new international agreements so that together, we can raise the calibre of cyber security further. Moreover, the Netherlands will be presiding over of the European Union in the first half of 2016. Cyber security is one of the top priorities during that chairmanship. In Europe there's still a lot to be gained on this issue. We hope to make a considerable stride forwards, in both increasing cyber security and reducing cyber crime in Europe. The Cyber Security Council also provides a valuable contribution to this. '

MEER INTERNET-VEILIGHEID BEGINT BIJ BETER ONDERWIJS

GREATER INTERNET SECURITY STARTS WITH BETTER EDUCATION

Betere educatie is één van de topthema's waarover de Cyber Security Raad zich buigt in 2015. Oud-staatssecretaris van Onderwijs Tineke Netelenbos heeft een duidelijk idee waar het heen moet. 'Ik vind dat het onderwijs mensen moet opleiden voor de samenleving waarin zij straks een rol spelen. Dan is het logisch dat je jongeren opleidt om digivaardig te worden. Veiligheid hoort daarbij.'

Better education is one of the top themes concerning the Cyber Security Council in 2015. Former State Secretary of Education Tineke Netelenbos has a clear idea where this should be going. 'I believe that education should raise young people for the society in which they will later be playing a role. It is logical therefore that young people should become digitally skilled. Security is a part of that learning process.'

Niet goed genoeg

'We zitten in een transitie van een analoge naar een digitale wereld. Daar past bij dat ook het onderwijs die transitie maakt en jongeren goed voorbereidt op die digitale samenleving. De overheid maakt cyberonderwijs op dit moment nog niet zo belangrijk als taal of rekenen. Ik vind dat dit wel moet. We hebben in Nederland ontzettend veel dataverkeer en internetstart-ups. Ook doen we het goed in sectoren als de landbouw omdat we alles digitaliseren en automatiseren. De digitale techniek is belangrijk voor Nederland, we zijn er goed in. Dan is het toch heel vreemd dat we cyber in het onderwijs niet als een van de kernvakken zien.

Het Nederlandse onderwijs scoort internationaal best goed. Maar als het gaat om ICT en cyberveiligheid in het onderwijs, dan is dat nog behoorlijk vrijblijvend. We staan op de negende plaats in de EU. Dat is natuurlijk niet goed genoeg. Het onderwijs moet op drie niveaus verbeteren.'

1. Mediawijsheid in het basisonderwijs

'Landen als Finland voeden kinderen spelenderwijs op voor de digitale samenleving. Ik vind dat ook wij al in het basisonderwijs moeten beginnen met mediaopvoeding in de volle breedte. We moeten kinderen leren wat media en internet kunnen betekenen. In positieve, maar ook in negatieve zin. Er ligt daar een belangrijke taak voor het onderwijs. Je kunt dit niet alleen aan de ouders overlaten.'

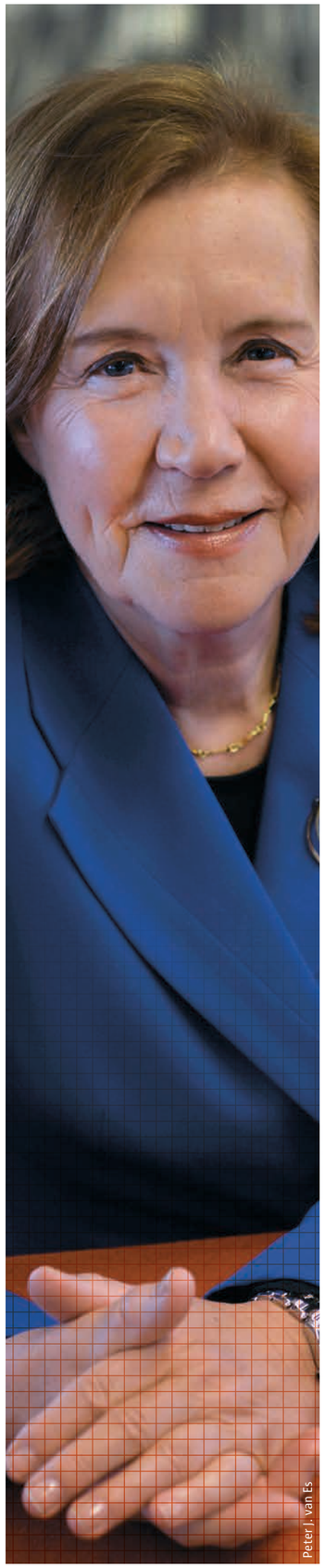
2. Enthousiasmeren in het voortgezet onderwijs

'Op dit moment wordt het vak informatica ontmanteld. Ik vind dat je het juist moet ombuigen tot vak dat jongeren opleidt om te functioneren in de digitale samenleving. Daar leren ze bijvoorbeeld coderen. Als je dit op een leuke manier aanbiedt, kun je jongeren enthousiast maken om een beroep te kiezen in de ICT. Er is een tekort aan instroming op de ICT-opleidingen. ICT heeft een 'nerdy' uitstraling. Maar je kunt hartstikke leuke dingen doen met computertaal, bijvoorbeeld spelletjes of apps maken. Als het vak goed gegeven wordt, kunnen we jongeren in het voortgezet onderwijs enthousiast maken voor een carrière in de ICT.
Maar ook veiligheid moet op het voortgezet onderwijs een permanent punt van aandacht zijn. Zo worden leerlingen zich bewust van de impact die het heeft als je de verkeerde dingen op het net zet. Dat is voor jongeren zelf belangrijk, maar ook voor het bedrijfsleven. Menselijk gedrag is vaak de zwakste schakel bij de beveiliging tegen cybercriminaliteit. Het is dus belangrijk dat toekomstige werknemers zich daar bewust van zijn. Sommige scholen doen al aan voorlichting, maar het gebeurt maar mondjesmaat. Het Ministerie van Onderwijs, Cultuur en Wetenschap moet scholen een aantrekkelijk programma over digiveiligheid aanbieden dat ze gemakkelijk kunnen invoeren.'

3. Vervolgopleidingen

'De docent is een rolmodel. Op dit moment zijn er niet genoeg docenten in het voortgezet onderwijs die verstand hebben van ICT en cybersecurity. Daarom moeten we deze disciplines verplicht stellen op lerarenopleidingen. Ook kunnen we na- en bijscholingscursussen aanbieden aan docenten in het veld. Door het onderwijs aan docenten te verbeteren, kunnen we ICT-vakken later verplicht stellen in het voortgezet onderwijs. Zo brengen we de motor op gang.

Op andere vervolgopleidingen wordt cyber niet overal goed onderwezen. Als we naar de IT-opleidingen op de technische universiteiten kijken, dan staan we er goed voor. Er is meer een probleem bij het beroepsonderwijs. Nog niet alle opleidingen onderwijzen voldoende digitale vaardigheden. Dat moet beter. Je kunt immers geen beroep meer verzinnen waarin ICT geen rol van betekenis speelt.'



Peter J. van Es

TINEKE NETELENBOS
Chairperson of ECP, Platform for the Information Society
Digital Champion for the Netherlands

Not good enough

'We're currently in the middle of a transition from an analogue to a digital world. That means that education must also make that transition and prepare today's youth for the digital society. At present the government is not making cyber education as important as language or arithmetic. However, I believe it should be doing that. We have an incredible amount of data communication and internet start-ups in the Netherlands. We're also doing well in sectors such as agriculture, because we digitalise and computerise everything. Digital technology is important for the Netherlands and we're good at it, which means it's strange that we don't have cyber in the education system as one of the core subjects.

Dutch education scores pretty well in international league tables. But when it comes to IT and cyber security in education, then that is a particularly voluntary matter. We're in ninth position in the EU. And that is, of course, not good enough. Education must be improved on three levels.'

1. Media wisdom in primary school education

'Countries such as Finland educate children for life in the digital society through play. I believe that we should start at primary school level with media education in its fullest terms. We need to teach children what the media and the internet can mean for us. Both in the positive as well as the negative senses. There is an important task ahead for the education sector. You cannot simply leave this to the responsibility of the parents.'

2. Creating enthusiasm in secondary school education

'Currently this subject is being disassembled. I believe that it should be changed instead into a subject that educates the youth how to function in the digital society. This would include teaching them how to code. If you offer this in an interesting manner, then you can make these young people enthusiastic about choosing an occupation in IT. At present there is a shortage of people entering IT courses. IT still has rather a 'nerdy' image. But it's possible to do really interesting things with computer language, for example creating games or apps. If the subject is taught well, then we can make the secondary school students enthusiastic about a career in IT.

But security must also become a permanent point of consideration in secondary school education. This would teach students to become aware of the impact when you upload the wrong things to the internet. That's important for the young people themselves, of course, but also for the business world. People often behave by way of being the weakest link when it comes to security versus cyber crime. It is therefore important that future employees are aware of that. Some schools have already started with giving information, but this only happens to a small extent. The Ministry of Education, Culture and Science should offer an attractive programme about digital security that the schools can implement easily.'

3. Further education

'The teacher as role model. There are currently not enough teachers at secondary school level who have a genuine understanding of IT and cyber security. That is why we need to make these disciplines obligatory within the teacher training programmes. We can also offer refresher courses and extra training to teachers in the field. By improving the education for teachers, at a later stage we will be able to make the IT subjects obligatory within secondary school education. That's how we could start up the engine.

As a subject, cyber is not taught consistently well in other extra training programmes. If we look at the IT courses at the technical universities, however, then we're doing well. This is more of a problem in the area of professional education. Not all of the courses provide sufficient education in digital skills. That must be improved. After all, you cannot think of any profession today in which IT does not play a role.'

Hollandse Hoogte

By **Martin Beumer**, Work Group Evaluation of Cyber Security in the Chain

(The work group has representatives of: Shell, Gasunie, Gasunie Transport Services, Nuon, Tennet, Alliander and the NCSC.)

In zijn boek 'Blackout' beschrijft de Oostenrijkse schrijver Marc Elsberg in 2012 het horrorscenario: een weken durende energieblackout in heel Europa door een cyberaanval. Hoe realistisch is dit? Gasunie Transport Services (gastransport), Nuon (elektriciteitsproducent/leverancier), TenneT (elektriciteitstransport) en Alliander (gas- en elektriciteits-distributie) nemen, onder leiding van Shell en ondersteund door het NCSC, de uitdaging aan om deze potentiële bedreiging in kaart te brengen. *In his book 'Blackout' (2012), Austrian writer Marc Elsberg described a doom scenario: weeks of energy blackouts across Europe as a result of a cyber attack. How realistic is this scenario? Gasunie Transport Services (gas transport), Nuon (electricity producer/supplier), TenneT (electricity transport) and Alliander (gas and electricity distribution) take the challenge to map out this potential threat, coordinated by Shell and supported by the NCSC.*

ENERGIEPARTIJEN BRENGEN KWETSBAARHEDEN KETEN IN KAART

ENERGY PARTIES MAP OUT VULNERABILITIES

'Hoe kwetsbaar en weerbaar is onze energievoorziening eigenlijk voor cyberaanvallen?' Die vraag wordt door de Cyber Security Raad gesteld aan de energiesector. Koninklijke Shell heeft een vertegenwoordiger in de Raad en die besluit de uitdaging aan te gaan. Shell benadert vier partijen die elk een onderdeel in de energieketen vormen om deze vraag te beantwoorden. Hierbij komen zij al snel tot de conclusie dat voor een analyse van een dermate complexe keten geen enkele panklare methode op de plank ligt. 'We moesten al rennen, terwijl we nog leerden lopen', omschrijft Henrie Mathijssen (TenneT) de uitdaging. De aanpak moest gaandeweg worden ontwikkeld, terwijl de analyse al werd uitgevoerd.

Kijkje in de keuken

Voor de analyse van dreigingen moet eerst de hele energieketen in beeld worden gebracht. Voor de deelnemende partijen betekent dit,

'How vulnerable and resilient is our energy supply after a cyber attack?' The Cyber Security Council asked the energy sector this question. Royal Shell has a representative on the Council who decided to take on this challenge to answer the question. Shell asks four parties which each form part of the energy chain to help answer this question. They soon reach the conclusion that there is no ready-made method for analysing such a complex chain. 'We were learning how to run before we could walk,' says Henrie Mathijssen (TenneT) when asked to describe the challenge. The approach had to be developed throughout the process, while the analysis was already being carried out.

A look behind the scenes

If you want to be able to carry out an analysis, you first have to map out the entire energy chain. For the participating parties, this means that they let the other parties take a look behind the scenes. Mapping out the entire chain at all parties involved is mainly thanks to the efforts of experts from the organisations involved, because there are very few people who have an overall picture. In the end, a picture was created at four levels:

1. the physical gas and electricity supply,
2. the administrative process,
3. the organisations' own IT systems and their direct links,
4. the shared IT equipment and services.

In the physical process, the possible scenarios for disruption and failure with the associated impact have been identified and analysed. The next step was to zoom in on threats and vulnerabilities, particularly on

uiteraard onder afspraken over vertrouwelijkheid, dat zij een kijkje in hun keuken geven aan de andere partijen aan tafel. Het in kaart brengen van de hele keten bij alle deelnemende partijen is mede te danken aan de inzet van deskundigen uit de eigen organisaties, want er zijn maar weinig mensen die een totaaloverzicht hebben. Uiteindelijk is er een beeld opgesteld op vier niveaus:

1. de fysieke gas- en elektriciteitsvoorziening;
2. het administratieve proces;
3. de eigen IT-systemen en hun directe koppelingen;
4. gemeenschappelijke IT-middelen en –diensten.

In het fysieke proces zijn de mogelijke scenario's voor onderbreking en verstoring met hun impact geïnventariseerd en geanalyseerd. Daarna is ingezoomd op dreigingen en kwetsbaarheden, met name op de koppelpunten tussen de partijen en hun gemeenschappelijke componenten. Deze zijn weer in verband gebracht met de scenario's in het fysieke proces. 'Je kunt het binnen je eigen organisatie wel op orde hebben, maar uiteindelijk is de keten zo sterk als de zwakste schakel', merkt Paul Bloemen (Gasunie) op.

Uitgaan van het onwaarschijnlijke

'Het is van belang om heel onwaarschijnlijke of niet voor de hand liggende mogelijkheden te analyseren', voegt Aad Dekker (Alliander) toe. 'Door de samenwerking kunnen we naar onderlinge afhankelijkheden en gecombineerde scenario's kijken en over de partijen heen inventarisaties uitvoeren. Zo weten we nu welke IT-producten en –diensten bij meerdere partijen in gebruik zijn. Dat geeft extra inzicht, omdat het aanvallen hiervan mogelijk extra aantrekkelijk is voor kwaadwillenden.' Uit de analyse blijkt dat er geen aanleiding is voor het nemen van extra maatregelen tegen cyberaanvallen. De kwetsbaarheid van de keten wordt voldoende klein geacht en de veerkracht voldoende groot. Wel houden de deelnemende partijen contact met elkaar en zullen ze periodiek een nieuwe analyse uitvoeren.

Methodiek beschikbaar

Het is waardevol gebleken om met alle partners vanuit het risico van cyberaanvallen naar de keten te kijken. Dat levert belangrijke nieuwe inzichten op, die gebruikt kunnen worden voor het verbeteren van de cybersecurity van onze energievoorziening. Volgens het projectteam valt deze exercitie uiteindelijk best mee en weegt de opbrengst zeker op tegen de inspanning. 'Wij nodigen dan ook partijen in andere ketens uit om deze exercitie uit te voeren. De beschreven methodiek stellen we aan anderen ter beschikking via het Nationaal Cyber Security Centrum en de Cyber Security Raad.'

the links between the parties and their joint components. These were subsequently connected to the scenarios in the physical process. 'Things may be in order within your own organisation, but in the end the chain is as strong as its weakest link,' says Paul Bloemen (Gasunie).

Starting from the improbable

'It is important to analyse highly improbable or highly unlikely scenarios,' adds Aad Dekker (Alliander). 'Cooperation has enabled us to go over our mutual dependencies and combined scenarios and carry out assessments that affect all parties. We now know which IT products and services several of our parties use. This gives us further insight, as attacking them could possibly be more appealing to malicious parties.' The analysis has shown that there is no reason for taking extra measures against cyber attacks. The chain's vulnerability is assessed as sufficiently small and resilience as sufficiently high. However, the participating parties maintain contact with each other and will carry out new analyses periodically.

Methods available

It was proven to be useful to jointly view the chain from the perspective of risk of cyber attacks. It has yielded important new insights, which can be used to improve cyber security in our own energy supply. According to the project team, the amount of effort was not too great, in hindsight, while the results more than outweighed the efforts. 'We would like to urge other parties in other chains to do the same. We have described the methods we used to make them available via the NCSC and the Cyber Security Council.'

ARJEN DORLAND

Executive Vice President Technical and Competitive IT Shell

VEILIGE SYSTEMEN DANKZIJ SAMENWERKING

SECURE SYSTEMS THANKS TO COLLABORATION

Bij multinationals staan vestigingen over de hele wereld continu met elkaar in verbinding. Een goede beveiliging van de IT-systemen is voor hen cruciaal. Voor een veilige digitale omgeving is 'samenwerking' het toverwoord, weet Arjen Dorland.

Within multinationals their branches over the whole world are continually connected with each other. Good security of the IT systems is crucial for them. 'Collaboration' is the magic word when it comes to a secure digital environment, Arjen Dorland knows.

Concurrerende bedrijven zijn van nature niet geneigd om belangrijke informatie met elkaar te delen. Als het om cybersecurity gaat, maken multinationals hierop een uitzondering. Dorland: 'We willen niet concurreren op het gebied van cybersecurity. Als je over dit onderwerp kennis uitwisselt, dan worden we daar allemaal beter van.'

Multinationals werken niet alleen samen aan een veilige digitale werkomgeving. Ze betrekken ook bedrijven in de keten bij het proces. 'Voor multinationals is het belangrijk dat de beveiliging op orde is bij organisaties waarmee ze samenwerken.'

Om de veiligheid in de keten goed in beeld te krijgen, deed de Cyber Security Raad een proef met ketenanalyse. Hierbij werd de digitale veiligheid van organisaties in een hele productreis doorgelicht. Dorland is enthousiast over de aanpak. 'Normaal gesproken bekijkt iedereen de veiligheid van zijn eigen organisatie. Maar wanneer je al die afzonderlijke organisaties in een lijn achter elkaar bekijkt, dan zie je weer andere veiligheidsrisico's. Ik denk dus zeker dat deze ketenanalyses nuttig zijn.'

Initiatieven als de ketenanalyse tonen volgens Dorland de grote meerwaarde van de Cyber Security Raad. 'In tegenstelling tot andere landen werken overheid, academici en bedrijfsleven in Nederland samen. Dat is uniek en heel effectief. De Cyber Security Raad is geen praatclub, maar toont daadkracht. Er is al veel bereikt, waar we als multinational heel veel aan hebben.'

Competitive businesses by their nature are not inclined to share important information with each other. When it comes to cyber security, however, multinationals make an exception to this. Dorland: 'We do not want to compete in the area of cyber security. If you share knowledge on this subject, then we all benefit from that.'

Multinationals do not only collaborate on a secure digital working environment. They also involve businesses in the chain during the process. 'It is important for multinationals that the security is in good order at the organisations with which they collaborate.'

In order to gain a clear picture of the security in the chain, the Cyber Security Council tested a chain analysis. This entailed analyzing the digital security of organisations throughout the whole trajectory of the products. Dorland is enthusiastic about the approach. 'Normally speaking, everyone looks at the security of their own organisation. But when you look at all those separate organisations in row behind each other, then you come across different risks. I definitely believe that these chain analyses are worthwhile.'

Initiatives such as chain analysis, according to Dorland, demonstrate the immense added value of the Cyber Security Council. 'Contrary to what occurs in other countries, the government, academics and the business community work together in the Netherlands. That is unique and extremely effective. The Cyber Security Council is not a discussion group, it shows dynamism instead. Much has already been achieved, which is highly valuable to multinationals.'

Shell International B.V

World Forum

By **Wilma van Dijk**, Director of Cyber Security and deputy National Coordinator for Counterterrorism and Security at the Ministry of Security and Justice

Met de implementatie van de Nationale Cyber Security Strategie versterken we de digitale weerbaarheid van Nederland en zetten we de koers voor de Nederlandse cybersecurity-aanpak. Publieke en private partijen werken daarbij nauw samen om veiligheid, vrijheid en maatschappelijke groei te realiseren. *With the implementation of the cyber security strategy, we have increased the Netherlands' digital resilience, while setting the course for the Dutch cyber security approach. Public and private parties work closely together to achieve security, freedom and societal growth.*

CYBER SECURITY RAAD:

EEN ONAFHANKELIJK EN KRITISCH ADVISEUR VOOR DE NEDERLANDSE CYBERSECURITY-AANPAK

CYBER SECURITY COUNCIL: INDEPENDENT AND CRITICAL ADVISOR FOR THE DUTCH CYBER SECURITY APPROACH

Sinds de verschijning van 'Cyber Security Beeld Nederland 2014' is het duidelijk dat de tijdsdimensie van ICT-implementatie een belangrijke rol speelt bij cybersecurity. De houdbaarheidsdatum van software- en hardwareveiligheid blijkt inherent beperkt. Zelfs wanneer producenten en organisaties een veilig product ontwikkelen en opleveren, ontwikkelen aanvallers zich minstens net zo snel en is het niet de vraag óf maar wannéér er kwetsbaarheden in een veilig systeem onderkend worden. Als gevolg daarvan zien we in het cybersecurity-beeld dat verouderde systemen een groeiende kwetsbaarheid vormen. Hoe gaan we om met dit soort uitdagingen? En hoe zorgen we voor een veilige toekomst in het digitale domein? Dit soort vragen kunnen alleen beantwoord worden in een publiek-privaat-wetenschappelijk discours; een constatering die vanaf de start van de Nederlandse cybersecurity-aanpak centraal heeft gestaan. De Cyber Security Raad is voor mij daarin een belangrijke toetssteen en adviseur. Door zijn onafhankelijkheid en kritische blik houdt de Raad de Nederlandse aanpak scherp en levert zo een wezenlijke bijdrage aan een veilige digitale samenleving.

Global Conference on Cyber Space

Het kader voor een veilige digitale samenleving wordt geschetst in de Nationale Cyber Security

The publication of the 'Cyber Security Assessment Netherlands 2014' made it clear that the temporal dimension of ICT implementation plays an important role in cyber security. The expiry date of software and hardware security appears to be inherently limited. Even if companies and organisations develop and provide a safe product, attackers just as easily develop new methods, which leads to the question not if but when vulnerabilities in safe systems will be discovered. The result is that the Cyber Security Assessment Netherlands has identified outdated systems as increasing vulnerabilities. How do we handle these challenges? And how do we ensure a safe future in the digital domain? These questions can only be answered in a public-private academic discourse, which has been the central focus of the Dutch cyber security approach from the start. I believe the Cyber Security Council is an important sounding board and advisor. Its independence and critical view keeps challenging the Dutch approach towards excellence, thus contributing greatly to a safe digital society.

Global Conference on CyberSpace

The framework for a safe digital society is outlined in the National Cyber Security Strategy 2 from 2013. In cooperation with its international partners, the Netherlands aims for a safe and open cyber domain in which the opportunities of information and

VERBINDING IS DE KERN VAN ONZE SAMENWERKING

CONNECTION IS AT THE HEART OF OUR COOPERATION

Strategie 2 uit 2013. Nederland zet samen met haar internationale partners in op een veilig en open cyberdomein, waarin de kansen die digitalisering onze samenleving biedt volop worden benut, dreigingen het hoofd worden geboden en fundamentele rechten en waarden worden beschermd. De samenhang tussen deze driehoek 'veiligheid, vrijheid en maatschappelijke groei' moet tot stand komen in een open dialoog tussen alle publieke, private en wetenschappelijke partijen, zowel nationaal als internationaal. Om deze dialoog te creëren en internationale coalities te vormen, organiseert Nederland dit jaar de internationale conferentie 'Global Conference on Cyber Space' (GCCS), waar de toekomst van het digitale domein centraal staat. Hierop aansluitend wordt tijdens deze conferentie aandacht besteed aan verhogen van het niveau van operationele centra in andere lidstaten ('CERT Maturity'). Tegelijkertijd past de thematiek van de GCCS ook als opmaat naar het EU-voorzitterschap van Nederland in 2016, waarin cyber een belangrijk thema zal zijn. Beide momenten waarbij we ons inzetten om het streven uit onze tweede nationale strategie waar te maken: Nederland is in Europa één van de koplopers in cybersecurity. En daar ben ik als directeur Cyber Security trots op.

Verbindende samenwerking

Ik ben nu één jaar directeur Cyber Security. Als ik terugkijk naar het afgelopen jaar, dan zie ik dat de ontwikkelingen razendsnel gaan. Wij als overheid moeten daarom snel schakelen. Dat vergt lenigheid die soms niet van nature aanwezig is. Hoewel de term publiek-privaat in zichzelf een tegenstelling lijkt te bevatten – er staat immers een streepje tussen – ervaar ik dat niet zo. Vanuit verschillende bloedgroepen onderkennen we hetzelfde gemeenschappelijke belang: een veilige digitale samenleving als een safe place to do business. Het Nationaal Cyber Security Centrum (NCSC) speelt daarin een belangrijke rol als centraal samenwerkingsplatform in de Nederlandse aanpak. Het NCSC fungeert als CERT voor de Rijksoverheid én als faciliterend orgaan voor het vitale bedrijfsleven. Vanuit het NCSC coördineren we incidenten én bieden we expertise en advies. Daarom werken we publiek-privaat samen én faciliteren we private samenwerking. Voor mij is de term publiek-privaat daarom geen koppeling van twee uitersten. Voor mij laat het verbindingsstreepje zien dat verbinding de kern van onze samenwerking is. Dit is een moderne manier van beleid maken en veiligheid creëren in een netwerksamenleving, die past in het unieke cyberdomein.

communication technologies (ICT) are fully seized, threats are countered and fundamental rights and values are protected. The correlation of this triangle of 'security, freedom and societal growth' has to be established in an open dialogue between all public, private and academic parties, both on a national and international level. In order to enable this dialogue and the formation of international coalitions, the Netherlands will organise this year's edition of the international conference 'Global Conference on CyberSpace' (GCCS), which will focus on the future of cyberspace. As a follow-up, attention is paid during the conference to increasing the level of operational centres in other Member States ('CERT Maturity'). The theme of the GCCS is also a prelude to the Dutch EU Presidency in 2016, which will highlight cyber issues. These are two opportunities where we aim to fulfil our commitments from our second national strategy: the Netherlands as one of the leaders in the area of cyber security in Europe. And, as the Director of Cyber Security, this makes me proud.

Connecting cooperation

I have been the Director of Cyber Security for one year now. When looking back at the past year, I see that developments have been taking place at break-neck speed. We, as a government, have to act quickly. This requires some level of flexibility, which we do not always have in our DNA. Although the term public-private seems to be contradiction in terms, highlighted by the hyphen, I do not see it that way. The various parties all recognise the same common interest: a safe digital society as a *safe place to do business.* The National Cyber Security Centre (NCSC) plays an important role in this as the central platform for cooperation in the Dutch approach. The NCSC is both CERT for the national government and the facilitating body for the vital business sector. From the NCSC, we coordinate incidents and provide expertise and advice. That is the reason why we embrace public-private cooperation and facilitate private cooperation. Therefore, I do not see the term public-private as a combination of two extremes. To me, the hyphen indicates that 'connection' is at the heart of our cooperation. This is a modern way of making policy and creating security in a networked society, which fits in with our unique cyber domain.

De IT-sector en online diensten bieden veel economische kansen voor Nederland. Cybersecurity is daarbij zowel een belemmering als een kans, vindt Mark Dierikx van het Ministerie van Economische Zaken. *The IT sector and online services offer many economic opportunities for the Netherlands. Cyber security is thereby both an obstacle as well as an opportunity, Mark Dierikx of the Ministry of Economic Affairs considers.*

CYBERSECURITY: BEPERKING ÉN KANS

CYBER SECURITY: LIMITATION AND OPPORTUNITY

MARK DIERIKX
Director-General Energy, Telecom and Competition Ministry of Economic Affairs

Cybersecurity is een beperking

'Nieuwe IT-toepassingen kunnen ons enorm ontzorgen. Toch kunnen we niet alle innovaties voluit toepassen, omdat we steeds moeten letten op de veiligheid. Waarom kan het ministerie niet zomaar in de cloud werken? Omdat eerst technologie moet worden ontwikkeld om die cloud af te schermen. We moeten continu alert zijn op de schending van onze informatie-uitwisseling. Dat beperkt ons.'

Cybersecurity is een kans

'Nederland is een voorloper op het gebied van IT. We hebben met de Amsterdam Internet Exchange (AMS-IX) het grootste internetknooppunt ter wereld en goede infravoorzieningen. Dit maakt ons een aantrekkelijke vestigingsplaats voor internetondernemingen. Dit kunnen we alleen blijven als bedrijven kunnen rekenen op een betrouwbaar elektriciteitssysteem en een veilig netwerk. Om dit te waarborgen, is cybersecurity een belangrijke randvoorwaarde. Betrouwbaarheid van telecominfra en het gebruik van internet is wezenlijk voor economische groei.'

Ook is cybersecurity een nieuwe markt en het biedt daarmee kansen. Bedrijven kunnen namelijk oplossingen bedenken voor digitale dreigingen. Op dit gebied timmert Nederland al aardig aan de weg, met bijvoorbeeld bedrijven als Fox-IT en het securitycluster van bedrijven The Hague Security Delta. Economische Zaken stimuleert onderzoek en innovaties waarbij online security en privacy uitgangspunten zijn. Daarbij vinden we het extra interessant als digitale veiligheid niet zorgt voor extra handelingen. We streven naar veilige oplossingen waarbij je niet hoeft in te leveren op het gebruiksgemak.

Cyber Security Raad: balans tussen beperkingen en kansen

'De Cyber Security Raad zorgt met de multidisciplinaire samenstelling voor een balans tussen de twee kanten. In het verleden letten partijen als Economische Zaken vooral op de kansen van ICT en cyber, terwijl anderen vooral veel aandacht hadden voor het gevaar dat schuilt in IT-innovaties en de bescherming die moest worden geregeld. Nu we meer samen optrekken, komt er binnen de partijen meer begrip voor beide belangen. De Cyber Security Raad zorgt zo voor evenwicht.'

Cyber security is a limitation

'New IT applications can relieve us enormously of particular concerns. However, we aren't able to fully apply all the available innovations, since we constantly need to keep one eye on security. Why is the ministry unable to work in the cloud just like that? Because the technology must first be developed to protect that cloud. We need to be continually alert to violations of our information exchange. That limits us.'

Cyber security is an opportunity

'The Netherlands is a front-runner in the area of IT. With the Amsterdam Internet Exchange (AMS-IX) we have the largest internet junction in the world, as well as good infrastructure provisions. This makes us an attractive place for establishing internet businesses. We can only retain this position if businesses can rely on a reliable electricity system and a secure network. In order to safeguard this, cyber security is an important precondition. Reliability of telecom infrastructure and the use of the internet are fundamental to economic growth'.

Cyber security is also a new market and thereby offers opportunities. Businesses can create solutions, for xample, for digital threats. The Netherlands is making good strides in this area, for example with businesses such as Fox-IT and the security cluster of businesses The Hague Security Delta. The Ministry of Economic Affairs stimulates research and innovations, whereby online security and privacy are the basic principles. In addition, we believe it to be of extra interest if digital security does not necessarily lead to extra actions. We are striving to find secure solutions, whereby you are not required to reduce the ease of use.

Cyber Security Council: balance between limitations and opportunities

'With its multidisciplinary composition, the Cyber Security Council provides a balance between the two sides. In the past, parties such as the Ministry of Economic Affairs looked mainly at the opportunities provided by IT and cyber, while others mainly paid attention to the dangers concealed in IT innovations and the protection that needed to be arranged. Now that we're working together, there is far more understanding within the parties for both interests. In this way the Cyber Security Council provides a balance.'

De nationale krijgsmacht bestaat al lang niet meer uitsluitend uit militairen in schepen, gepantserde voertuigen en straaljagers. Na land, lucht, water en ruimte is cyber de vijfde dimensie waarin de strijd wordt uitgevochten. ‘Soms is het verstoren of vernietigen van een informatiesysteem belangrijker dan het vernietigen van een raketwerper’, weet Rob Bauer, directeur Plannen bij Defensie. *For a long time now, the national armed forces do not only comprise members of the military in ships, armoured vehicles and fighter jets. After maritime, land, air and space, cyber has become the fifth dimension in which the battle can being fought. ‘Sometimes, disrupting or destroying an information system is more important than destroying a rocket launcher’, Rob Bauer, Director of Plans at the Ministry of Defence knows.*

CYBER: DE VIJFDE DIMENSIE VAN DEFENSIE

CYBER: THE FIFTH DIMENSION OF DEFENCE

Digitale technologie heeft de manier waarop strijdkrachten opereren in korte tijd veranderd. Niet alleen bevatten wapens en voertuigen steeds geavanceerdere digitale technologie, ook verandert de verhouding tussen staatslegers en burgerbewegingen tijdens conflicten. ‘Door de ontwikkelingen in de IT is kennis gedemocratiseerd’, legt Bauer uit. ‘Vroeger wisten de staat en de krijgsmacht meer dan de bevolking van een land. Tegenwoordig beschikken ook burgers over veel informatie, met name dankzij internet.’ Voor relatief weinig geld kun je een app (laten) maken waarmee je een telefoon kunt overnemen, of met een iPad een wapensysteem kunt bedienen. ‘Vroeger hadden alleen staten geld om digitale systemen van een tegenstander te beïnvloeden. Nu kunnen ook burgers relatief goedkoop aan dit soort kennis en middelen komen. Soms is het verstoren of zelfs vernietigen van een informatiesysteem belangrijker dan het vernietigen van een raketwerper.’

Cyber verandert bovendien het strijdtoneel, legt Bauer uit. ‘Vroeger vond een oorlog plaats op een duidelijke locatie. Tegenwoordig kan het gebeuren dat je strijdt tegen een groep in Mali, maar digitaal wordt aangevallen door een sympathisant in Nederland. Steeds vaker wordt naast een conventionele oorlog een cyberoorlog gevoerd. Oorlog is hybride geworden, en de strijd is daardoor minder overzichtelijk.’

Nieuwe realiteit

Defensie heeft de Nederlandse krijgsmacht aangepast aan de nieuwe realiteit. ‘Cyber is onderdeel van en ondersteunend aan al onze operaties. Het is niet belegd in een apart krijgsmachtsonderdeel. Binnen de gehele Defensieorganisatie houden steeds meer militairen zich met cyber bezig,’ aldus Bauer.

De in 2012 opgestelde Defensie Cyber Strategie dicteert dat daarbij primair aandacht is voor de bescherming van eigen systemen. Het speciale cybersecurity-centrum DefCERT monitort 24 uur per dag of iemand probeert in te breken in de systemen van de krijgsmacht. Daarnaast werkt Defensie samen met het Nationaal Cyber Security Centrum aan de digitale weerbaarheid van Nederland.

Ook houdt Defensie zich sinds kort bezig met de ontwikkeling van offensieve cybercapaciteiten. Het in september 2014 opgerichte Defensie Cyber Commando beschermt de eigen wapensystemen voor, tijdens en na operaties. Daarnaast ondersteunt deze nieuwe eenheid de conventionele strijd. ‘Als je vroeger een gebied wilde aanvallen, moest je eerst de radar- en luchtverdedigingssystemen uitschakelen door ze te bombarderen. Voor vliegers was dit een gevaarlijke job. Nu probeer je de systemen plat te leggen met een hack. Zo kan offensieve cyber een conventionele operatie ondersteunen.’

ROB BAUER

Rear-Admiral RNLN Rob Bauer
Director of Plans – Netherlands Ministry of Defence

Samenwerken

Om de cyberactiviteiten succesvol te maken, werkt Defensie samen met andere organisaties. ‘We willen goede hackers, maar je kunt niet Anonymous bellen met de vraag of je een opleiding bij ze kunt volgen. We werken daarom samen met gerenommeerde cybersecuritybedrijven.’ Medewerkers van Defensie gaan een jaar in opleiding bij een bedrijf, en leren daar vaardigheden die ze vervolgens kunnen toepassen voor de krijgsmacht.

Bauer is enthousiast over de samenwerking met bedrijven, die hij ook terugvindt bij de Cyber Security Raad. ‘Wat heel krachtig is in Nederland, is dat we ons vanaf het begin hebben gerealiseerd dat cyber geen grenzen heeft. Of je nu een overheidsinstelling, bank of wetenschappelijk instituut bent, we hebben allemaal met dezelfde dreiging vanuit het cyberdomein te maken. Buitenlandse collega’s zijn jaloers op de manier waarop we samenwerken in de Raad. We denken niet in zuilen, we praten met elkaar. En, heel belangrijk, we delen ervaringen. Ook pijnlijke. Dat maakt het zo krachtig. We kunnen veel leren van elkaar, en dat vertalen naar de eigen organisatie. Zo leren wij vanuit de Cyber Security Raad hoe we Defensie op het gebied van cyber nog beter kunnen maken.’

Digital technology is rapidly changing the way in which forces operate. Not only do weapons and vehicles contain advanced digital technology, but the relationship between armed forces and civilian organizations during conflicts is also changing. ‘Developments in the IT sector have democratised knowledge’, Bauer explains. ‘The State and the armed forces used to know more about the population of a country than anyone else. However, citizens now have a great deal of information available to them thanks to smart phones and the internet.’ For a relatively small amount of money you can make an app, or have one made, with which you can take over a telephone, or operate a weapon system from an iPad. ‘Not too long ago only States had the money and the knowledge to influence the digital systems of an opponent. Now citizens, too, can get hold of this type of knowledge relatively cheaply. Sometimes, disrupting or destroying an information system is more important than destroying a rocket launcher.’

Moreover, cyber changes the battlefield, Bauer explains. ‘In former times, a war took place at a clear location. Nowadays it may be that you are fighting against a group in Mali, but attacks are carried out digitally by a sympathiser in the Netherlands. Increasingly often we see a cyber war being fought alongside a conventional war. War has become hybrid, which means that the struggle is now far less clear-cut.’

New reality

Defence has adjusted the Dutch armed forces to the new reality. ‘Cyber will increasingly form a part of all aspects of our operations. It is not housed in a separate branch of the armed forces. Within the whole Defence organisation, increasing numbers of military staff are involved with cyber,’ according to Bauer.

The Defence Cyber Strategy formulated in 2012 dictates that attention is giving primarily thereby to the protection of our own systems. The special cyber security centre DefCERT monitors twentyfour hours a day whether someone is trying to break into the systems of the armed forces. In addition, Defence works together with the National Cyber Security Centre on the digital resilience of the Netherlands.

Defence is also becoming involved in the development of offensive cyber capabilities. The Defence Cyber Command, which was set up in September 2014, protects our own weapon systems before, during and after operations. In addition, this new unit supports the conventional way of ending conflicts. ‘Previously, when you wanted to attack a particular area, you first had to incapacitate the radar and air defence systems by bombing them. That was a dangerous job for pilots. These days you try to bring down the systems using a hack. In this way offensive cyber can support a conventional operation.’

Collaboration

In order to ensure that cyber activities are successful, Defence works together with other organisations. ‘We want to have good hackers, but you can’t just phone Anonymous with the request to follow a course with them. Therefore we work together with reputable cyber security companies.’ Employees from Defence spend a year in training with a company, and there they learn the skills which they can subsequently apply for the benefit of the armed forces.

Bauer is enthusiastic about the collaboration with other companies, which he also sees at the Cyber Security Council. ‘What is really strong in the Netherlands, is that from early on we realised that cyber is without borders. Whether you are a government body, a bank or a scientific establishment, we are all confronted with the same threats from the cyber domain. Foreign colleagues are sometimes jealous of the way in which we collaborate at the Cyber Security Council. We don’t think in separate blocks: we talk to each other. And, most importantly, we share our experiences. Even the painful ones. That makes it so powerful. We can learn so much from each other, and then translate that to suit our own organizations. This means that we gain knowledge from the Cyber Security Council as to how we at Defence can make improvements in the area of cyber.’

GERRIT VAN DER BURG
Procurator General
Public Prosecution Service

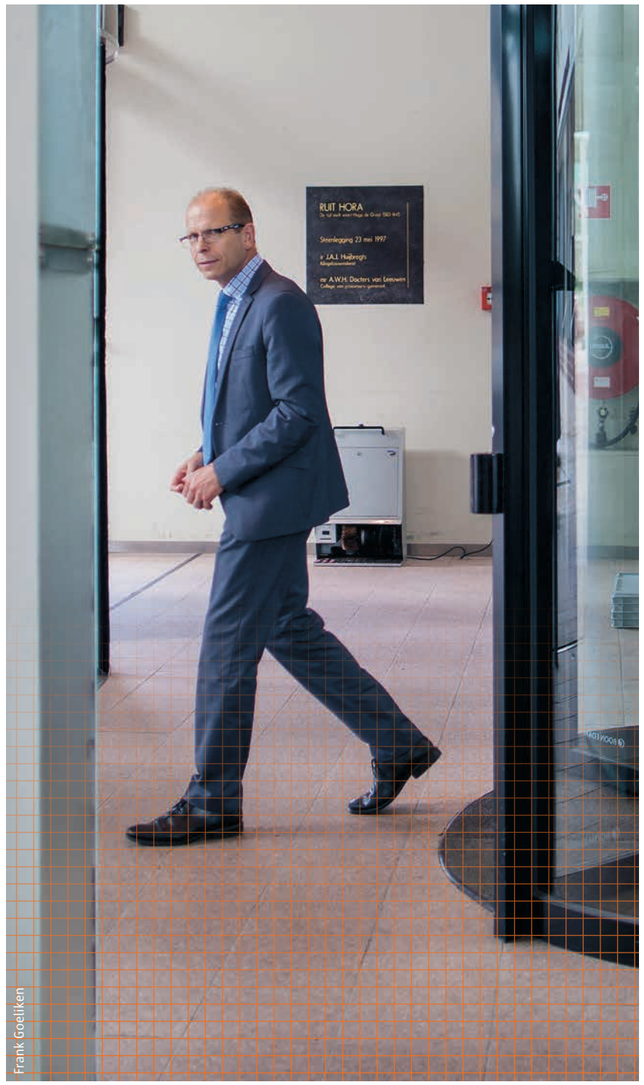
‘STRAFRECHT IS NIET ZALIGMAKEND’

‘CRIMINAL LAW IS NOT THE UNIVERSAL REMEDY’

‘Cybercrime is in korte tijd één van de belangrijkste vormen van criminaliteit geworden. Het ontwikkelt zich met een enorme snelheid en hevigheid. Voor de bestrijding van cybercrime is strafrecht niet zaligmakend. Samen met andere partijen proberen we vooral ook cyberdreigingen af te wenden en te voorkomen. Het strafrecht kan worden gebruik als ‘optimum remedium’, passend in een arrangement van maatregelen van weerbaarheid, preventie en repressie.

Superspecialisten

De specialisten van het Team High Tech Crime van de Nationale Politie doen op landelijk niveau onderzoeken naar de belangrijkste cyberbedreigingen onder verantwoordelijkheid van gespecialiseerde officieren van justitie. Bijvoorbeeld naar aanvallen op de vitale infrastructuur, nationale veiligheidsissues en grote hacks. Daarnaast ontwikkelt elke regio eigen specialisten die zich bezig houden met de bestrijding van cybercrime. Zo ontwikkelt onze kennis zich in de diepte en in de breedte.



Frank Goeliken

Opsporing bemoeilijken

Binnen de opsporing hebben we veel uitdagingen. Zo zien we dat de versleutelingstechnieken steeds moeilijker te kraken zijn. Én dat deze hoogwaardige technieken voor steeds meer mensen bereikbaar worden. Ze wordt de opsporing dubbel uitgedaagd. Moeten leveranciers op dit punt beperkingen worden opgelegd? Of druist dat te veel in tegen vrijheid van ondernemen en de vrijheid van het individu? Het is een hoogst actuele discussie binnen de driehoek veiligheid, vrijheid en economisch belang.

Veiligheid afdwingen

Dit soort discussies voeren we in de Cyber Security Raad. Er is een groot gezamenlijk belang om het cybercriminelen zo moeilijk mogelijk maken. Wat kunnen we elk daaraan bijdragen? Met begrip en respect voor alle belangen proberen we een goed evenwicht te vinden. En inderdaad, dat is niet altijd gemakkelijk. Toch ben ik optimistisch, want kijk naar de auto-industrie. Auto’s waren 25 jaar geleden ook niet zo veilig als nu. Die veiligheid is deels afgedwongen door de overheid, maar de belangrijkste innovaties kwamen uit de industrie zelf. Ze werd daarbij kritisch gevolgd door de consumenten-organisaties. We staan pas aan de vooravond van een dergelijk proces voor cyber.

Duurzaam ondernemen

Ik zie digitale weerbaarheid als een logisch onderdeel van duurzaam ondernemen. Net zo logisch als milieuverantwoord ondernemen en als onderdeel van de totale ‘compliance’. We moeten ons dus nog bewuster worden van de risico’s. Bedrijven kunnen we bijvoorbeeld vragen hun cybersecurity te verantwoorden in hun jaarverslag. Ook dit soort maatregelen kan bijdragen aan meer bewustwording.’

Hollandse Hoogte

‘Within a short space of time, cyber crime has become one of the most important forms of criminality. It is developing at enormous speed and intensity. Criminal law is not the universal remedy for combating cyber crime. Together with other parties we are mainly trying to avert and prevent cyber threats. Criminal law can be used as the ‘optimal remedy’, as one element in an arrangement of measures of resilience, prevention and repression.

Super-specialists

The specialists in the Team High Tech Crime of the National Police Force carry out investigations at a national level into the most important cyber threats under the responsibility of specialised public prosecutors. They work on attacks, for example, on the vital infrastructure, national security issues and large hacks. In addition, each region develops its own specialists who are involved in combating cyber crime. This helps us to develop our knowledge broadly and in depth.

Hindering detection

We face a great number of challenges in detection. We see, for example, that the encryption techniques are becoming increasingly difficult to crack. Moreover, these high level techniques are becoming available to increasing numbers of people. This means that the detection is doubly challenged. Should limits be imposed on suppliers in relation to this point? Or does that conflict too much with the freedom to do business and the freedom of the individual? This is a highly topical subject within the triangle of security, freedom and economic interests.

Enforcing security

This is the type of discussion that we carry out in the Cyber Security Council. There is a very large mutual interest in making cyber crime as difficult as possible. What can each of us contribute to that? We do our best to find a good balance, while maintaining respect and understanding for all interests. And that is indeed not always easy. Still, I am optimistic; take for example the car industry. Twenty-five years ago cars were far less safe than what they are now. That safety was partly enforced by the government, but the most important innovations came from the industry itself. They were watched with a critical eye by the consumer organisations. We are now on the eve of such a process within the cyber world.

Sustainable business practices

I see digital resilience as a logical part of sustainable business practices. Just as logical as environmentally responsible business practices and part of the total compliance. Therefore we need to become even more aware of the risks. We could, for example, ask businesses to give an explanation of their cyber security in their annual reports. These types of measures can also contribute to greater awareness.’

De nationale inlichtingendienst is een van de organisaties die de digitale veiligheid van Nederland nauwlettend in de gaten houden. 'We moeten ons zorgen maken', vindt Rob Bertholee, hoofd van de AIVD. Hij deelt deze informatie in de Cyber Security Raad. *The national intelligence service is one of the organisations that keeps a very close eye on the digital security of the Netherlands. 'We need to be concerned', thinks Rob Bertholee, head of the General Intelligence and Security Service. He shares this information in the Cyber Security Council.*

'WE ZIJN IN NEDERLAND SOMS TE NAÏEF'

'SOMETIMES IN THE NETHERLANDS WE ARE TOO NAIVE'

Wat doet de AIVD aan cybersecurity?
'Wij houden ons bezig met complexe, langdurige dreigingen in cyberspace. Het gaat dan om aanvallen die als doel hebben om de veiligheid van de staat aan te tasten of de samenleving te ontwrichten. Wij doen onder meer onderzoek naar digitale spionage en sabotage. Ook geven we gevraagd en ongevraagd advies over cybersecurity aan organisaties in de vitale sector.'

Waar komt de dreiging vandaan?
'De aanvallen waar wij ons mee bezighouden, zijn vaak gesponsord door staten. We kijken bijvoorbeeld naar China, Rusland en ook landen als Iran. Maar ik ben ervan overtuigd dat alle landen, of ze nu meer of minder gecivitiliseerd zijn, zich met cyberspionage bezighouden vanaf het moment dat ze toegang hebben tot cyberinfrastructuur.'

Is er ook dreiging vanuit het terrorisme?
'We weten dat terroristische organisaties de capaciteit hebben om internet in te zetten. De vraag is of zo'n organisatie ook een terroristische daad kan plegen via internet. Bijvoorbeeld het openzetten van sluizen. We sluiten niet uit dat dit kan.'

Hoe staat Nederland ervoor qua cyberveiligheid?
'Internet dringt steeds meer door in de samenleving. Mensen gebruiken steeds meer mobiele applicaties en bij bedrijven zie je dat er steeds meer op afstand wordt gewerkt. Dat maakt je kwetsbaarder voor spionage. Ik denk dat de grote bedrijven in de vitale sector zich voldoende bewust zijn van de risico's die ze lopen. Of ze daarmee ook de risico's onder controle hebben, is niet zeker. Sommige bedrijven doen het hartstikke goed, en bij anderen is er ruimte voor verbetering. In algemene zin onderschatten we in Nederland de risico's van de digitale ruimte. We zijn in een aantal opzichten te naïef.'

Moeten we ons zorgen maken?
'Ja, dat vind ik wel. Als internet een steeds groter deel van ons leven gaat uitmaken, dan moet je je zorgen maken als je de bescherming daartegen niet op orde hebt.'

Waar ligt voor u de grens tussen veilige cyber en voldoende privacy voor iedereen?
'Dat zijn twee illusies. De ene is veilige cyber, de ander is dat iedereen zijn privacy kan bewaren. Als je van de AIVD vraagt dat we voorkomen dat er een terroristische aanslag plaatsvindt, dan moet je tegelijkertijd accepteren dat we middelen gebruiken die inbreuk maken op de privacy. Maar daar waar wij inbreuk maken op de privacy, is dat in verhouding met het doel dat we ermee dienen.'

Waarom is het belangrijk dat de AIVD deelneemt aan de Cyber Security Raad?
'De AIVD kan informatie inbrengen die de andere partijen niet hebben. Als AIVD hebben we bijzondere bevoegdheden: we mogen bijvoorbeeld hacken en afluisteren. Daarnaast zijn we internationaal ingebed. De digitale ruimte is grenzeloos, dus de samenwerking in internationaal verband is heel belangrijk. Tot slot kan de AIVD ook buiten de digitale ruimte informatie inwinnen. We kunnen bijvoorbeeld met bronnen praten en agenten inzetten. De combinatie van die methodes, dat is onze kracht.'

Wat is de toegevoegde waarde van de Cyber Security Raad voor de AIVD?
'We kunnen eruit leren. Bijvoorbeeld over de problemen waar bedrijven uit de vitale sector tegenaan lopen, of de gedachteontwikkeling over beveiliging versus privacy. De Raad is er niet alleen om praktisch naar bedrijven toe te gaan om het bewustzijn te vergroten. Hij is er ook om conceptueel en beleidsmatig na te denken en advies te geven bij het ontwikkelen van de Cyber Security Strategie.'


Lenny Oosterwijk

ROB BERTHOLEE

Director-General General Intelligence and Security Service (AIVD)

What does the General Intelligence and Security Service do in relation to cyber security?
'We are involved with complex, long-term threats in cyberspace. This entails attacks with the objective of having a detrimental effect on the security of the State or disrupting society. Part of our work is to investigate digital espionage and sabotage. We also give advice about cyber security, both requested as well as unsolicited, to the vital sectors.'

Where does the threat originate?
'The attacks with which we are concerned are often sponsored by States. We're looking, for example, at China and Russia, as well as countries such as Iran. But I'm convinced that all countries, however advanced they may be, are busy with cyber espionage from the moment that they have access to the cyber infrastructure.'

Is there also a threat coming from terrorist quarters?
'We know that terrorist organisations have the capacity to deploy the internet. The question is whether such an organisation is also able to commit a terrorist act via the internet. For example, by opening navigational locks. We don't exclude this as a possibility.'

What is the situation regarding cyber security in the Netherlands?
'The internet is becoming an increasingly common factor in society. People are using increasing quantities of mobile applications and you see within businesses the growth in work carried out remotely. This makes us more vulnerable to espionage. I think that the large businesses involved in the vital sectors are sufficiently aware of the risks they face. Whether they have those risks under control, however, is another question. Some businesses are doing very well, whereas others still have room for improvement. Generally speaking, though, in the Netherlands we underestimate the risks of the digital space. We are simply too naive in a number of ways.'

Do we need to be concerned?
'Yes, I believe so. If the internet takes over an increasingly large part of our lives, then you need to be concerned if the protection required is not good enough.'

Where do you see the border between secure cyber and sufficient privacy for everyone?
'Those are two illusions. One is secure cyber, the other is that everyone can safeguard their own privacy. If you want the General Intelligence and Security Service to prevent a terrorist attack from occurring, then you must accept at the same time that we need to use means that involve a certain invasion of privacy. However, where we do invade privacy, that is balanced with the objective we are thereby serving.'

Why is it important that the General Intelligence and Security Service participates in the Cyber Security Council?
'The General Intelligence and Security Service can contribute information that the other parties don't have access to. At the General Intelligence and Security Service we have special authorities: we are permitted, for example, to hack and to tap phones. In addition, we are internationally embedded. The digital space is without borders, hence the collaboration at an international level is extremely important. Finally, the General Intelligence and Security Service is also able to gather information outside of the digital space. We're able, for example, to talk to different sources and to deploy our agents. The combination of all those methods is our strength.'

What does the General Intelligence and Security Service provide in the way of added value to the Cyber Security Council?
'We can learn from it. For example, about the problems that the businesses in the vital sectors come up against, or the development of thinking about security versus privacy. The Council is not only there to address businesses in a practical way about increasing awareness. It is also there to think in conceptual and policy-based terms and to give advice in the development of the Cyber Security Strategy.'


ANP

By **Prof. Bart Jacobs**,
Professor of Computer Security,
Radboud University Nijmegen
and **Prof. Herbert Bos**,
Professor of Computer Security,
VU Amsterdam

Moderne ICT-systemen zijn zo enorm complex, dat fouten en beveiligingsrisico's onvermijdbaar zijn. Maar wat doe je als je een fout in software tegenkomt? Voor de hand liggend is de fabrikant te informeren. Alleen blijken die de afgelopen decennia niet altijd adequaat te reageren en fouten niet onmiddellijk te herstellen. Een alternatief is de gevonden fout publiek maken. De druk op fabrikanten wordt daarmee flink verhoogd om snel te reageren. In Nederland is een tussenweg verheven tot beleid: responsible disclosure and repair.

Modern ICT systems are so immensely complex that security risks are unavoidable. But what are you supposed to do with software vulnerabilities? The most logical thing to do is inform the software company. However, over the past decades, these companies have not always responded adequately and immediately fixed such vulnerabilities. An alternative is to make software faults public. This increases the pressure on the companies to respond quickly. The Netherlands has converted the middle course into policy: responsible disclosure and repair.

RESPONSIBLE DISCLOSURE AND REPAIR

Het risico van een fout publiceren, is het gevaar van misbruik door kwaadwillenden. Toch blijkt uit ervaring dat fabrikanten op dat moment vaak pas genegen zijn op de juiste wijze te reageren en hun software te repareren. Onder security-onderzoekers en (goedwillende) hackers is een tussenweg ontstaan die responsible disclosure genoemd wordt: meld de fouten en kwetsbaarheden vertrouwelijk aan de fabrikant, maar zeg daarbij dat de fout binnen redelijke termijn publiek gemaakt zal worden.

De leidraad

De Mifare Classic is een chip waarvan er wereldwijd miljarden verkocht zijn. In 2008 ontdekten academische security-onderzoekers grote zwakheden in de chip. Ze hebben dit direct vertrouwelijk gemeld en planden een wetenschappelijke publicatie. De chipfabrikant NXP ging naar de rechter om een publicatieverbod af te dwingen, maar zonder succes.
Deze rechtszaak heeft de verhouding tussen onderzoekers en fabrikanten op scherp gezet. Daarom stond het direct op de agenda van de Cyber Security Raad, na zijn oprichting in 2011. De brede samenstelling van de Raad leidt tot een strategische aanpak gericht op samenwerking, niet op confrontatie. De Nederlandse overheid heeft hierop in 2013 een leidraad 'Responsible Disclosure' gepubliceerd. Daarin worden bedrijven aangemoedigd om zelf aan te geven: (a) hoe

The risk associated with disclosing a fault is that parties with malicious intent may abuse the situation. Yet, experience has shown that companies only quickly fix software vulnerabilities after public disclosure. Security researchers and (well-intentioned) hackers have agreed on a compromise that is dubbed responsible disclosure: report the faults and vulnerabilities to the company in a confidential manner, with the added statement that the fault will be made public within a reasonable term.

The guideline

The Mifare Classic is a chip that has sold billions worldwide. In 2008, academic security researchers discovered that the chip had major vulnerabilities. They immediately informed the company in a confidential manner and planned a scientific publication. Chip manufacturer NXP went to court to enforce a publication ban, but failed.
This case has driven a wedge between researchers and manufacturers. It was therefore put on the agenda of the Cyber Security Council immediately following its inception in 2011. The broad composition of the Council results in a strategic approach aimed at cooperation instead of on confrontation. The Dutch government responded in 2013 by publishing a 'Responsible Disclosure' guideline. The guideline encourages companies to take the initiative and state: (a) how vulnerabilities can be reported confidentially, (b) that such reports will be taken seriously and, provided there is no abuse, (c) that this will not lead to (civil)

DE BREDE SAMENSTELLING VAN DE RAAD LEIDT TOT EEN STRATEGISCHE AANPAK GERICHT OP SAMENWERKING, NIET OP CONFRONTATIE.

THE BROAD COMPOSITION OF THE COUNCIL RESULTS IN A STRATEGIC APPROACH AIMED AT COOPERATION INSTEAD OF ON CONFRONTATION.

kwetsbaarheden vertrouwelijk gemeld kunnen worden, (b) dat zulke meldingen serieus opgepakt zullen worden en, mits geen sprake is van misbruik, (c) niet leiden tot (privaatrechtelijke) aangifte. Het Openbaar Ministerie houdt echter nadrukkelijk ruimte voor een eventuele eigen strafrechtelijke aanpak van de melder.

De praktijk

Verschillende Nederlandse bedrijven volgen nu de leidraad. De ervaringen van telecombedrijf KPN zijn ronduit positief. De meldingen hebben bij KPN onbekende zwakheden naar boven gebracht, die tot grote interne veranderingen en betere beveiliging hebben geleid. Opmerkelijk is dat KPN zelf pleit voor verbetering van de positie van de melder, omwille van grotere opbrengst van de regeling[1]: '... we definitely see the benefit of a responsible disclosure program but agree that current legal legislation governing this area can be discouraging and potentially leave the notifier exposed.' De grote banken begonnen gelijktijdig met hun responsible disclosure-beleid. Voormalig lid van de Cyber Security Raad René Steenvoorden (Rabobank): 'De honderden meldingen die de banken sinds 2013 krijgen, betreffen veel kleine of reeds bekende zaken. Tijdige en accurate reactie vergt weliswaar capaciteit, maar dit meedenken is het ons waard.' IT-journalist Brenno de Winter suggereert om hackers meer zekerheid te geven: 'Laat het Openbaar Ministerie een bindende richtlijn openbaren over hun vervolgingsbeleid in deze.'

De evaluatie

Het feit dat Nederland officieel beleid heeft op het gebied van responsible disclosure is, zover bekend, uniek in de wereld. Bedrijven zijn positief, maar hackers zijn terughoudender. Van begin af aan is er kritiek geweest op de eenzijdige nadruk op verplichtingen voor melders, zonder zekerheden. Een agressief bedrijf kan een goedwillende melder nog steeds juridisch hard aanpakken. Dit is een reëel probleem: in 2014 legde een Londense rechter op verzoek van Volkswagen een publicatieverbod op aan Nederlandse onderzoekers. De strafrechtelijke vervolging van melders is in de praktijk een kleiner risico. Desalniettemin is een evenwichtiger naam voor het beleid: 'responsible disclosure and repair'. Dit benadrukt de verplichting om gesignaleerde problemen op te lossen!

1. Zie: Rob Kuiters, *Engaging with the security community at large - Lessons from Responsible Disclosure*. In: *Cyber Security Perspectives 2013*, http://www.kpn-cert.nl/CybersecurityPerspectives2013.pdf

same time, major banks introduced their responsible disclosure policy. René Steenvoorden (Rabobank), former member of the Cyber Security Council: 'The hundreds of reports banks have been receiving since 2013 mainly concern small or known cases. A timely and accurate response does require resources, but we think the contribution is worth it.' IT journalist Brenno de Winter has suggested giving hackers more certainty: 'Have the Public Prosecution Service publish a binding guideline about their prosecution policy in these matters.'

The evaluation

The Dutch official policy on responsible disclosure is unique in the world, as far as is known. Companies are positive, while hackers are more reserved. There has been criticism from the start on the one-sided emphasis on notifiers' obligations, while they do not have any certainties. An aggressive company is still able to come down hard on a notifier in a legal procedure. This is a real problem: in 2014, a London court imposed a publication ban on Dutch researchers, at the request of Volkswagen. Criminal prosecution of notifiers is a much smaller risk in practice. Nevertheless, a more balanced name for the policy would be: 'responsible disclosure and repair'. This name underlines the obligation to actually solve identified issues!

legal action. However, the Public Prosecution Service has reserved room for criminal prosecution of notifiers.

Actual practice

Various Dutch companies have started to follow the guideline. The experiences of telecom company KPN have been unanimously positive. The reports have revealed major vulnerabilities at KPN, which in turn have led to major internal changes and improved security measures. It is striking that KPN itself is now an advocate of improving the position of notifiers, because they see the greater benefits of the program[1]: '... we definitely see the benefit of a responsible disclosure program but agree that current legal legislation governing this area can be discouraging and potentially leave the notifier exposed.' At the

1. See: Rob Kuiters, Engaging with the security community at large - Lessons from Responsible Disclosure. In: Cyber Security Perspectives 2013, http://www.kpn-cert.nl/CybersecurityPerspectives2013.pdf

By **Mr. Lodewijk van Zwieten**, National Prosecutor for cyber crime, the Netherlands

Cyberaanvallen worden professioneel uitgevoerd en het is moeilijk te ontdekken wie erachter zit. Wie moet er dan optreden tegen zo'n aanval? De beste first response is eensgezind overheidsoptreden in samenwerking met private partijen. There is no I in team. *Cyber attacks are being executed in a professional manner and it is increasingly difficult to establish the identity of the attackers. Which parties are thus best equipped to act against such an attack? The appropriate first response is a unified government action in cooperation with private parties. There is no I in team.*

WIE TREEDT OP TEGEN EEN CYBERAANVAL?

WHO WILL ACT AGAINST A CYBER ATTACK?

Wie treedt op tegen een cyberaanval? Dit attributievraagstuk is steeds lastiger te beantwoorden. Recente grootschalige cyberaanvallen, zoals op Sony, laten zien dat het niet eenvoudig is om ze te kwalificeren als criminaliteit, ideologische of oorlogsdaad. Aanvallen worden zorgvuldig uitgevoerd en uiterlijke kenmerken als identiteit van het doelwit en het gebruikte 'cyberwapen' geven onvoldoende aanknopingspunten.

Iedereen gelijk

Reden voor die moeilijke attributie is het toenemende gebruik van geavanceerde afschermtechnieken en krachtige cyberwapens. Anders dan bij kinetische wapens is dit niet gereguleerd. Of het nu gaat om statelijke actoren, beroepscriminelen of ideologische aanvallers; ze beschikken allemaal over hetzelfde arsenaal aan cyberwapens. Als gevolg daarvan bedienen cybercriminelen zich van 'Advanced Persistent Threats', terwijl dat voorheen een sterke indicator was voor betrokkenheid van statelijke actoren. Aan de kant van de aanvallers is steeds meer sprake van een level playing field.

Mismatch

Het speelveld aan de kant van slachtoffers en overheid is allesbehalve vlak. Het ontbreken van duidelijke aanwijzingen over de herkomst en het motief van een grootschalige cyberaanval,

Who is best equipped to act against a cyber attack? It is becoming increasingly difficult to attribute such attacks. Recent large-scale cyber attacks, like the one on Sony, show that it is not easy to qualify them as acts of crime, nor ideologically motivated acts or acts of war. Attacks are meticulously carried out and external characteristics like the identity of the target and the cyber weapon used, offer insufficient leads to formulate a proportionate response.

Level playing field

One of the reasons why it has become so difficult to attribute cyber attacks is the increased use of advanced detection prevention techniques. Another is that both state sponsored actors, professional criminals and ideologically motivated attackers all have the same powerful cyber weapons at their disposal. As a result, Advanced Persistent Threats, previously a strong indicator of state actor involvement, are now being deployed for criminal purposes. The playing field on the attackers' side has become quite level.

Mismatch

The playing field on the side of the victims and the government is everything but level. The lack of clear indications about the origin of and motive behind a large-scale cyber attack hinder the determination of a legal framework for an intervention. At worst this may lead to a mismatch between

Een medewerkster van de gemeente Weert zit achter een schrijfmachine nu de computers van de instelling buiten gebruik zijn door een virus. Zeker dertig instellingen, waaronder gemeenten, bedrijven en universiteiten, zijn op 9 augustus 2012 getroffen door het computervirus XDocCrypt/Dorifel. Het Nationaal Cyber Security Centrum onderzoekt de meldingen en probeert de omvang in kaart te brengen.

An employee of the municipality Weert uses an old fashioned type-writer since the computers are out of order due to a virus. At least thirty institutions; municipalities, companies, universities, have been hit by a computer virus XDocCrypt/Dorifel. The National Cyber Security Centre is investigating the reports and tries to establish the scope of the attack.

ANP

EEN EFFECTIEVE FIRST RESPONSE OP GROOTSCHALIGE CYBERAANVALLEN BESTAAT UIT EENSGEZINDE SAMENWERKING TUSSEN OVERHEDEN.

AN EFFECTIVE FIRST RESPONSE TO LARGE-SCALE CYBER ATTACKS STARTS WITH UNIFIED COOPERATION BETWEEN GOVERNMENT BODIES

belemmert het vaststellen van juridische kaders waarbinnen geïntervenieerd dient te worden. In het ergste geval levert dat een mismatch op tussen aanval en reactie. Dan wordt er bijvoorbeeld met militaire kracht gereageerd, terwijl de aanval afkomstig is van een criminele dader. Of opsporingsbevoegdheden worden ingezet, terwijl die geen effect hebben op een statelijke actor.

Eensgezind

Een effectieve first response op grootschalige cyberaanvallen bestaat uit eensgezinde samenwerking tussen overheden. Ze gaan te werk vanuit hun eigen taakstelling, maar creëren een gezamenlijke informatiepositie. Dat biedt de mogelijkheid om gecoördineerde maatregelen te nemen om aanvallen af te slaan, daders te identificeren en een proportionele reactie vorm te geven. Daarbij dient gestreefd te worden naar een optimale en rechtmatige combinatie van ieders bevoegdheden, met inachtneming van de eisen die in Nederland gelden voor samenwerking tussen overheden. Als voorbeeld gelden de politiediensten en krijgsmachten van veel landen. Onder voorwaarden mogen zij elkaar wederzijdse bijstand verlenen.

Scenario's

Om het handelingsperspectief van overheidspartijen te kunnen bepalen en op elkaar af te kunnen stemmen, is het zinvol om in de voorbereiding op cyberaanvallen te werken met hypotheses. In dit kader worden herkomst en motief van de aanval, identiteit van het doelwit, directe en potentiële gevolgen van de aanval uitgewerkt in scenario's. Hierin staat omschreven welke overheden worden ingezet, wat van hen verwacht mag worden en welke partij in the lead is. Bij de aanpak van grootschalige cyberaanvallen in Nederland zijn met deze werkwijze goede ervaringen opgedaan.

Privaat

Naast samenwerking tussen overheden dienen ook private partijen betrokken te worden in de strijd tegen cyberaanvallen. Zij kennen hun eigen handelingsperspectief, wat een waardevolle combinatie met overheidshandelen kan zijn. In preventieve zin mag van de private sector verwacht worden dat hij (door de overheid voorgeschreven) maatregelen neemt die de maatschappelijke weerbaarheid verhogen. En dat hij zich wapent tegen de mogelijkheid dat systemen ongewild worden ingezet om andere partijen aan te vallen.

Teamwork

In een optimale publiek-private samenwerking wordt het handelen van de samenwerkende partijen bepaald door het effect dat men wil bereiken. De gezamenlijke aanpak en verantwoordelijkheden worden binnen wettelijke kaders vastgelegd in rules of engagements, zodat iedereen weet waar hij aan toe is en wat hij moet doen. Om binnen de grenzen van de rechtstaat zover te komen, dienen publieke en private partijen over hun eigen schaduw heen te stappen. Want de aanpak van grootschalige cyberaanvallen is teamwork. There is no I in team. Alleen dan kan het speelveld ook aan de kant van slachtoffers en overheden vlak worden.

---

attack and response, whereby military force is used in response to a criminal attack or inadequate investigative powers are used against a state actor.

Unified

An effective first response to large-scale cyber attacks starts with unified cooperation between government bodies, where all actors work from their own assigned responsibilities, but available information is pooled and shared with the collective. This creates better opportunities for coordinated actions to ward off attacks, identify perpetrators and shape a proportionate response. Government bodies should then aim to reach an optimal and lawful combination of their authorities, within the applicable legal framework. Police services and armed forces of many countries for example are already allowed to help one another under certain conditions.

Scenarios

To establish and reconcile the possibilities and extent of a government cooperation in preparation for cyber attacks, it is useful to work with hypotheses about the attribution. Based on these hypotheses, the origin and motive of an attack, the identity of the target and direct and potential consequences of an attack are laid down in scenarios. These can describe which government body is to act, what is expected of them and which body is in the lead. This method has worked well in the Netherlands in dealing with large-scale cyber atacks.

Private parties

Government cooperation aside, private parties can have a key role in fighting cyber attacks. Interventions by private parties have significant added value to a government response. At a minimum, private parties may be expected to take certain actions to enhance society's resilience (directly or through their customers), and to prevent against criminal misuse of their services and computer systems in cyber attacks.

Team work

In an optimal private public partnership, the actions are determined by the desired outcome. Furthermore, the joint approach and shared responsibilities are laid down in a clear agreement and rules of engagement are set. This ensures that all parties know what is expected of them. To come to such an optimal cooperation, both public and private parties need to shrug off their reservations. Because fighting large-scale cyber attacks is team work. And there is no I in team. Only then can the playing field become truly level.

Foto: TenneT, Chris Parmarts

BEN VOORHORST

Chief Operational Officer TenneT

‘CYBERSECURITY MOET EEN NORMAAL ONDERDEEL VAN DE BEDRIJFSVOERING WORDEN’

‘CYBER SECURITY SHOULD BECOME A NORMAL PART OF BUSINESS OPERATIONS’

‘Energie is onmisbaar voor onze samenleving en daarom onderdeel van onze vitale infrastructuur. Net als bijvoorbeeld voedsel, drinkwater, geld en ICT. Ik neem vanuit het perspectief van de vitale sectoren deel aan de Cyber Security Raad. Voor hen is de continuïteit van hun bedrijfsprocessen cruciaal. Want zij moeten onder alle omstandigheden hun product kunnen leveren. Naast fysieke dreigingen is daar sinds een jaar of tien ook de cyberdreiging bijgekomen.

Vooruit kijken

De cyberwereld is een globale wereld. Zodra je het internet op gaat, zijn er geen grenzen meer. In de Cyber Security Raad kijken overheid, private sector en wetenschap gezamenlijk wat er op ons afkomt. We discussiëren over zaken die fundamenteel zijn, waar we het antwoord nog niet op hebben gevonden. We willen daarbij niet teveel focussen op de problemen van gisteren, maar juist vooruit kijken. Hoe transparant moet een bedrijf zijn bij een cyberincident? Welke data kunnen en willen bedrijven delen met de overheid? Moet de overheid kaders stellen of moeten bedrijven dat zelf doen? Hoe moet het strafrecht worden aangepast aan cybercriminaliteit? Het antwoord op die vragen moet uiteindelijk leiden tot internationaal toepasbare oplossingen.

Wijzere voorstellen

Door te overleggen in de Cyber Security Raad zorgen we ervoor dat de drie partijen niet tegenover elkaar staan in het publieke domein. De discussies zijn soms stevig, maar uiteindelijk willen we met elkaar dit belangrijke dossier vooruit helpen. Zodat we allemaal met wijzere voorstellen komen, ieder op zijn eigen werkveld. We willen immers geen onzinnige regels die schijnzekerheid creëren en voor ballast zorgen bij bedrijven en consumenten. Denk aan de cookiewetgeving.

We zijn ons de afgelopen jaren steeds bewuster geworden van cybersecurity, maar ik vrees dat de ontwikkelingen in de malafide wereld nog veel sneller gaan. Cybersecurity moet dus snel een normaal onderdeel worden van de bedrijfsvoering van elke organisatie. Dat is één van de uitdagingen voor de komende jaren.’

HOE TRANSPARANT MOET EEN BEDRIJF ZIJN BIJ EEN CYBERINCIDENT?

HOW TRANSPARANT SHOULD A COMPANY BE IN THE CASE OF A CYBER INCIDENT?

‘Energy is indispensable in our society and therefore electricity grids are part of our vital infrastructure. Just as, for example, food, drinking water, money and IT. I participate in the Cyber Security Council from the perspective of the critical infracture sectors. For those sectors, the continuity of their business processes is crucial. Because they must be able to deliver their products under all circumstances. Besides the physical threats, over the last ten years cyber threat has also been added to the equation.

Looking ahead

The cyber world is a global world. As soon as you go on the internet, all borders disappear. In the Cyber Security Council the government, the private sector and the science world look together at what is thrown at us. We discuss matters that are fundamental, to which we have not yet found the answers. This means not focusing too much on yesterday’s problems, but looking ahead instead. How transparent should a company be in the case of a cyber incident? Which data can businesses share with the government and which do they want to share? Should the government set frameworks or should businesses do that themselves? How should criminal law be amended in respect of cyber crime? The answer to those questions should in the end lead to internationally applicable solutions.

Wiser proposals

Through our discussions in the Cyber Security Council we ensure that the three parties are not in opposition in the public domain. The discussions are sometimes quite heated, but our goal is to help this important dossier to move forward. So that we can all offer wiser proposals, each in his or her own working field. After all, we do not want ridiculous rules that create a false sense of security and that simply provide extra ballast for businesses and consumers. Take, for example, the legislation regarding cookies.

We have become increasingly aware of cyber security over the last few years, but I fear that developments in the world of fraud and cyber crime are moving much faster. Cyber security should therefore become a normal part of the business operations of every organisation as soon as possible. That is one of the challenges facing us for coming years.’

Foto: ANP

‘Nederland kan de Digital Delta van Europa worden’, meent Bart Hogendoorn van Nederland ICT. Organisaties moeten zich dan wel bewust zijn van de risico’s. *‘The Netherlands could become the Digital Delta of Europe’, Bart Hogendoorn of Nederland ICT believes. Organisations must become aware of the opportunities but also of the risks.*

CYBERSECURITY IN DE BOARDROOM: DE WAL KEERT HET SCHIP

CYBER SECURITY IN THE BOARDROOM: THE COURSE OF THINGS WILL AUTOMATICALLY TAKE A DIFFERENT TURN


Clemens Rikken

BART HOGENDOORN
Chairman of Nederland ICT
Managing Director of HP Netherlands

In de berichtgeving over cybersecurity gaat het vaak over de gevaren van internet. Zijn er ook kansen?
‘Cyber biedt grote kansen voor Nederland. We kunnen de Digital Delta van Europa worden. We hebben alle kenmerken om een soort ICT-hub te zijn. Nederland is door regelgeving, ligging, scholing en infrastructuur een ideale proeftuin voor vernieuwing. In goedkope arbeid of grondstoffen kunnen we ons niet onderscheiden, we moeten het hebben van kennis. Bijvoorbeeld van de digitale wereld.’

Kunt u zich ook voorstellen dat mensen zich zorgen maken over de gevaren van internet en ICT?
‘Als je denkt dat je een eenvoudige transactie met de bank doet en je geld gaat naar Nigeria, dan kan ik me goed voorstellen dat mensen daarvan schrikken. Zowel voor consumenten als voor bedrijven kan de impact van onveilig internet enorm zijn. Daarom neem ik enthousiast deel aan de Cyber Security Raad. Ik zie het toch een beetje als de good guys tegen de bad guys. Je moet zorgen dat je continu voorop loopt.’

U werkt in de Cyber Security Raad samen met overheid en wetenschap. Welk nut ziet u in die samenwerking?
‘We moeten er samen voor zorgen dat de digitale omgeving werkt. Dat kunnen en willen we als ICT-bedrijven niet alleen doen. Het voordeel is dat de overheid, wetenschap en het bedrijfsleven net een andere blik op cybersecurity hebben. De Raad kan zorgen voor awareness, met internet of things als voorbeeld. En de raad brengt partijen bij elkaar, bijvoorbeeld voor responsible disclosure.’

U bent betrokken bij de werkgroep van de Cyber Security Raad over standaarden. Hoe kijkt u aan tegen de invoering van standaarden en de effectiviteit ervan?
‘Securitystandaarden zijn een leidraad om je organisatie digitaal veiliger te maken. Maar als je een standaard ziet als een afvinklijst, dan levert het geen veiligheid. Het is een dynamische wereld die snel verandert. Het is naïef om te denken dat het goedkomt als je maar voldoet aan een keurmerk. Laten we proberen om het aantal standaarden te beperken. Het gaat erom dat je als organisatie bewust met het thema bezig bent.’

Wat levert de werkgroep over standaarden dan op?
‘De werkgroep stelt een expertbrief op. Dit is een boodschap aan managers en bestuurders van organisaties, zodat ze zich meer bewust worden van de risico’s die er zijn en hoe standaarden – als een van de middelen – kunnen helpen om risico’s te beperken. Niet zodat bestuurders dan alles gaan dichttimmeren. Maar wel zodat ze begrijpen wat voor impact cyberaanvallen kunnen hebben op hun bedrijf.’

Zijn bestuurders van bedrijven zich voldoende bewust van de gevaren?
‘Ik denk het niet. Ik denk dat veel mensen in de boardroom nog geen idee hebben wat cybersecurity betekent. Zij denken: “Dat is een IT-dingetje.” Maar als je klanten weglopen omdat je niet goed met veiligheid omgaat, of als je intellectual property door buitenlandse concurrenten wordt gekopieerd, dan gaat dat direct het management aan. De wal keert het schip. Als er dingen fout gaan, dan hebben mensen plotseling in de gaten dat cybersecurity toch wel erg belangrijk is. Ik denk niet dat het kalf verdronken zal zijn, maar ik denk wel dat die af en toe een natte poot haalt.’

Reports about cyber security often mention the dangers of the internet. But are there opportunities as well?
‘Cyber offers great opportunities for the Netherlands. We could become the Digital Delta of Europe. We have all the characteristics for becoming a sort of IT hub. Due to regulations, situation, schooling and infrastructure the Netherlands is an ideal testing ground for modernisation. We may not be able to distinguish ourselves in terms of cheap labour or raw materials, but instead we need to make that distinction in terms of knowledge. For example, in the digital world.’

You can well imagine that people are concerned about the dangers of the internet and IT.
‘If you consider that you can carry out a simple transaction with the bank and your money goes to Nigeria, then I can easily imagine people being shocked by that. The impact of insecurities in the internet can be enormous for both consumers as well as businesses. That is why I’m an enthusiastic member of the Cyber Security Council. I see it rather in the way of the good guys against the bad guys. You need to make sure that you continually keep ahead.’

You work in the Cyber Security Council together with government bodies and scientific establishments. What advantage do you see in that collaboration?
‘Together we need to make sure that the digital environment works. As IT companies we cannot, nor do we want to do that on our own. The advantage is that the government, scientific establishments and the business community all have a slightly different view of cyber security. The Council can provide awareness, for example through the internet of things. Moreover, the Council brings parties together, for example for responsible disclosure.’

You are involved in the working group on standards of the Cyber Security Council. How do you view the introduction of standards and the effectiveness of these?
‘Security standards serve as a guideline for making your organisation more digitally secure. But if you simply view a standard as a checklist, then that does not provide security. It’s a dynamic world that is changing rapidly. It’s naive to think that all will be well if you simply comply with a quality mark. Let’s try to limit the number of standards. What’s involved is that your organisation should be consciously busy with the theme.’

What does the working group on standards provide?
‘The working group composes an expert letter. This contains a message to managers and directors of organisations, so that they become more aware of the risks that are out there and how standards, as one of the means, can help to limit the risks. This does not mean that directors can then close all the gaps. But rather that they understand the impact cyber attacks could have on their business.’

Do company directors have enough awareness of the dangers?
‘I don’t think so. I think that many people in the boardroom have simply no idea what cyber security means. They think: “That’s something for the IT department.” But if you start to lose your customers because you’re not handling security in a sensible manner, or if your intellectual property is being copied by foreign competitors, then that immediately affects the management. The course of things will automatically take a different turn. If things go wrong, then people suddenly realise after all that cyber security is very important indeed. I don’t think it’s too late yet, but I do think we’re still going to see some sorry victims.’

Hollandse Hoogte

By **Jos Schaffers**, Dutch Association of Insurers

Hoe voorkom je dat klantgegevens op straat belanden of online diensten in gevaar komen? Het is een vraag waar tal van bedrijven en overheden zich over buigen. Volgens het Verbond van Verzekeraars kunnen cyberverzekeringen helpen om bedrijven bewuster te maken van cybersecurity. Als verzekeraars eisen stellen aan de beveiliging én bedrijven voorbereiden op een cyberincident, snijdt het mes aan twee kanten. *How do you prevent customer data from being inadvertently disclosed or online services from being threatened? This is a question numerous companies and government bodies are struggling with these days. According to the Dutch Association of Insurers, cyber insurances could help with making companies more aware of cyber security. If insurers set security requirements and help companies prepare for cyber incidents, this would double the effectiveness.*

VERZEKERING HELPT BIJ BEWUSTWORDING CYBERSECURITY

INSURANCE HELPS TO RAISE CYBER SECURITY AWARENESS

Een datalek wordt soms veroorzaakt door menselijk of technisch falen, maar kan ook het gevolg zijn van een doelbewuste handeling van criminelen. Wat de oorzaak ook is, verzekeraars onderscheiden bij het bepalen van de potentiële schade twee categorieën: eigen schade (first party loss) en aansprakelijkheidsschade (third party loss). De eerste is het makkelijkst in te schatten: er wordt bijvoorbeeld gekeken hoeveel computers een bedrijf heeft staan, hoeveel bits aan data daarin omgaan, hoeveel uur het kost om alle opgeslagen gegevens opnieuw in te voeren of een back-up te plaatsen. Het inschatten van de mogelijke aansprakelijkheidsschade is een heel ander verhaal. Die schade hangt af van het type en aantal klanten/derden waarmee een bedrijf werkt en wat voor soort gegevens op straat komen te liggen. Zo zijn gezondheidsgegevens privacygevoeliger dan NAW-gegevens.

Cyberpolis nieuw fenomeen?

Cyberpolissen bieden dekking tegen zowel eigen schade als aansprakelijkheidsschade en kunnen zowel door grote als kleine bedrijven worden afgesloten. De polis an sich is niets nieuws: dekkingen voor eigen schade aan computersystemen worden al sinds de jaren tachtig aangeboden en aansprakelijkheidsdekkingen zijn vele malen ouder. Nieuw is wel dat de potentiële cyberschade met de komst van internet de afgelopen jaren is geëxplodeerd.

A data leak is sometimes caused by human or technological error, but may also be the result of a targeted action of criminals. Whatever the damages, insurers identify two categories when determining the potential losses: first party loss and third party loss. First party loss is easiest to assess: insurance companies take into account how many computers a company has, how many bits of data they store, how many hours it would take to re-enter all stored data or create a back-up, etc. Assessing third party loss, on the other hand, is much more difficult. Third party loss depends on the type and number of clients/third parties a company works with and on the type of data that would be disclosed. Health-related data, for example, are much more sensitive than name and address details.

Cyber insurance: a new phenomenon?

Cyber insurance covers both first party loss and third party loss and can be taken out by large and small companies alike. The insurance in itself is not new: coverage for first party loss to computer systems has been available since the 1980s and third party loss insurance is even older than that. The new feature, however, is that potential cyber damages have soared since the advent of the internet. Twenty years ago, one had to literally and physically stand next to a PC or server to be able to steal data, whereas stealing data can nowadays be done remotely without the victim ever noticing.

HOE GOED DE CYBERSECURITY IMMERS GEORGANISEERD IS, HET KAN ALTIJD EEN KEER MISGAAN.

NO MATTER HOW WELL CYBER SECURITY IS ORGANISED, THINGS CAN ALWAYS GO WRONG.

Twintig jaar geleden moest men voor het stelen van data nog fysiek naast een pc of server staan. Anno 2015 kan dat allemaal op afstand, zonder dat de getroffene er überhaupt iets van merkt. Dat maakt cyberschade een stuk weerbarstiger dan bijvoorbeeld water- of inbraakschade. Door bestaande ervaringen te combineren met de juiste kennis over cybersecurity komen verzekeraars echter al een heel eind. Bovendien zal de markt zijn werk doen: hoe meer partijen een cyberverzekering hebben, hoe meer ervaring verzekeraars zullen opdoen en des te groter wordt de kennis over cyberrisico's én de beheersing daarvan.

Risicomanagement

Dat laatste is belangrijk: een cyberpolis is méér dan een 'simpele fix' voor cyberrisico's. Het is onderdeel van gedegen risicomanagement, waarbij een bedrijf wordt getriggerd om de risico's goed in te schatten en na te denken over het beheersen daarvan. Niet voor niets stellen verzekeraars in de polisvoorwaarden doorgaans eisen aan de cybersecurity en geven ze advies over beveiligingsmaatregelen en het inschatten van de risico's. Verder denken verzekeraars graag mee over het anticiperen op een cyberincident. Hoe goed de cybersecurity immers georganiseerd is, het kan altijd een keer misgaan. Als klanten daarop zijn voorbereid, kan de schade vaak beter in omvang worden beperkt en daar heeft iedereen baat bij.

Publiek-privaat

Volgens het Verbond van Verzekeraars kunnen publieke en private partijen elkaar nog wel verder versterken. Zo bestaan er voor cyberveiligheid tal van standaarden, waardoor ondernemers door de bomen het bos niet meer zien. De overheid zou daar meer duidelijkheid in kunnen scheppen, door aan te geven wat de ondergrens is voor cybersecurity en wat er van bedrijven wordt verwacht.
Juist daarom is het Verbond zo blij met de Cyber Security Raad: de raad is een prachtig middel om kennis uit wetenschap, bedrijfsleven en overheden bij elkaar te brengen. Wat het Verbond betreft mag de raad nog veel meer op de voorgrond treden en ook het voortouw nemen in lastige discussies over het spanningsveld tussen veiligheid, privacy en commercie. Dat is niet altijd makkelijk, maar wél nodig om cyberschade beheersbaar te houden.

This makes cyber-related damage much more tricky than water or burglary damages. By combining existing experiences with the right knowledge about cyber security, insurers can come a long way though. The market will also learn from experience: the more parties have cyber insurance, the more experience insurers will gain, thus increasing knowledge about cyber risks and cyber risk management.

Risk management

Risk management is the key word here: cyber insurance is more than a simple fix for cyber risks. It is part of risk management, in which a company is triggered to properly assess the risks and consider and manage them. This is why insurers usually set cyber security requirements and give advice about security measures and risk assessment. Insurers are also more than willing to make proposals for anticipating cyber incidents. After all, no matter how well cyber security is organised, things can always go wrong. If customers are prepared for the event, the extent of damages can be limited , with benefits for all.

Public-private

According to the Dutch Association of Insurers, there is still room to improve the mutual effectiveness of public and private parties. There are so many cyber security standards that business owners can easily get overwhelmed. The government could provide more clarity by indicating the minimum requirement for cyber security and stating what is expected of companies. That is why the Association is so pleased with the Cyber Security Council: it is a good tool for bringing together knowledge from science, the business community and government bodies. The Association would like to see the Council be more prominent and take the lead in complex discussions about the interface of security, privacy and commerce. This is not always easy, but indispensable for keeping cyber-related damages manageable.

BAS EENHOORN
Digital Supervisor

DIGITALISERING BIJ DE OVERHEID:

VEILIGHEID IS VAN NATIONAAL BELANG

DIGITALISATION WITHIN THE GOVERNMENT: SECURITY IS OF NATIONAL IMPORTANCE

Overheidsinstanties digitaliseren. Hiervoor is een veilige en toekomstbestendige digitale infrastructuur noodzakelijk. Om dit in goede banen te leiden, heeft het kabinet vorig jaar de Digicommissaris aangesteld. Bas Eenhoorn werd in 2015 lid van de Cyber Security Raad. 'Bij de digitalisering is veiligheid een toponderwerp', benadrukt Eenhoorn. *Government bodies are digitalising. A digital infrastructure is needed for this, which is not only secure but which also takes account of future developments. In order to manage this well, last year the government appointed a Digital Supervisor. Bas Eenhoorn became a member of the Cyber Security Council. 'Security is one of the top subjects involved in digitalisation', emphasises Eenhoorn.*

'Tot nu toe digitaliseerden departementen, lokale overheden en uitvoeringsorganisaties als de Belastingdienst allemaal op hun eigen manier. Men liep elkaar voor de voeten en er was geen centrale sturing. Het kabinet heeft de Digicommissaris aangesteld om de verbinding te leggen tussen inhoud, sturing en financiën van de digitale voorzieningen. Mijn bureau heeft dus een regiefunctie. Daarnaast kan ik voorstellen doen aan een ministeriele commissie. Dit directe contact met besluitvormers maakt me slagvaardig. Die slagkracht is hard nodig om de digitalseringsambitie van ons land meer vaart te geven.

Digiprogramma

In maart presenteer ik aan de ministerraad een Digiprogramma. In dit plan staat hoe de overheid kan digitaliseren en in welk tempo. Het is een soort jaarplan van alle betrokkenen bij de digitale overheid. We ontwikkelen zo een samenwerking die uniek is voor overheidsinstanties. Die samenwerking is cruciaal om veilige,

'Up till now, the various different departments, local government and implementation organisations, such as the Tax and Customs Administration, all managed digitalisation in their own way. People were hampering each other and there was no central control. The government appointed the Digital Supervisor in order to make a connection between the content, control and financing of the digital provisions. Therefore my office has a directional function. In addition, I'm able to make proposals to a ministerial committee. This direct contact with decision-makers means my work can be efficient. That efficiency is greatly needed in order to provide the digitalisation ambition of our country with greater speed.

Digital Programme

I will be presenting a Digital Programme in March to the Cabinet. Set out in this plan will be how the government can digitalise and at what speed. It amounts to a sort of annual plan for all those involved in the digital government. In this way we are developing a collaboration, which is unique for government bodies. That collaboration is crucial in order to offer a secure, reliable and simple provision of services to our citizens and to businesses.

Part of the plan, for example, includes that citizens and businesses will no longer be required to pass on their details to individual government bodies. Systems must be coupled to each other so that will no longer be

Jurgen Hulskes

BURGERS MOETEN ZAKEN DIGITAAL MET DE OVERHEID KUNNEN REGELEN

CITIZENS SHOULD BE ABLE TO ORGANISE THEIR BUSINESS WITH THE GOVERNMENT DIGITALLY

betrouwbare en eenvoudige dienstverlening te bieden aan burgers en bedrijven.

Onderdeel van het plan is bijvoorbeeld dat burgers en bedrijven niet steeds aan individuele overheidsinstanties hun gegevens hoeven door te geven. Systemen moeten zo gekoppeld worden dat dit niet meer nodig is. Daarnaast werken we aan de modernisering van de dienstverlening van de overheid. Burgers moeten hun zaken digitaal met de overheid kunnen regelen, zonder dat een ambtenaar vraagt: “Wilt u dit formulier invullen en het ons per post toesturen?”
Ook komt er een nieuw systeem om je digitaal te identificeren. Het wordt een soort digitaal paspoort. De nieuwe toepassing moet veiliger en makkelijker worden dan DigiD. Het kan ook een nieuwe vorm krijgen, bijvoorbeeld een toepassing voor je mobiel met een code of je vingerafdruk. Dit middel kun je in de toekomst mogelijk niet alleen voor overheidsdiensten gebruiken, maar ook bij bedrijven of banken.

Veiligheid

Omdat de digitale overheid gebruikmaakt van generieke voorzieningen, is veiligheid van nationaal belang. Als kwaadwillenden inbreken of voorzieningen lam leggen, kunnen ze meteen veel schade aanrichten. Ik deel in de Cyber Security Raad waar ik mee bezig ben en praat over zaken waar ik tegenaan loop. Ik kan gebruikmaken van de kennis in de raad. De eerste kennismaking met de Cyber Security Raad heeft veel vertrouwen gegeven.’

necessary. Besides that, we’re working on the modernisation of the provision of services by the government. Citizens should be able to organise their business digitally with the government, without having a civil servant asking: “Would you complete this form and send it to us by post?”

A new system will also be introduced to enable people to identify themselves digitally. It will be a type of digital passport. The new application must be more secure and simple to use than DigiD. It may also come in the way of a new form, for example an application for your mobile phone with a code or your fingerprint. In the future you may be able to use this method not only for government services, but also for businesses or banks.

Security

Because the digital government makes use of generic provisions, security is therefore of national importance. If people with malicious intentions carry out break-ins or bring down provisions, they are immediately able to cause a great deal of damage. I keep the Cyber Security Council informed about what I’m currently concerned with and talk about the things I come up against. I’m able to make use of the knowledge available within the Council. My first meeting with the Cyber Security Council gave me a great deal of confidence.’

By **Prof. Eric Tjong Tjin Tai**,
Professor of Private Law, Tilburg University

Het recht wordt vaak gezien als een lange lijst van regels, geboden en verboden. In de dagelijkse praktijk loopt niemand die lijst na om te lezen wat hij wel of niet mag doen. Zo helpen en beschermen mensen elkaar op basis van wat in de gegeven situatie nodig is. Dat geldt ook voor ouders. Die luisteren naar de behoefte van hun kind en reageren daarop. De juridische term ‘zorgplicht’ sluit daarbij aan. Maar is het mogelijk om met zorgplichten cybercrime te bestrijden? Onderzoek moet dat uitwijzen. *Law is generally seen as a long list of rules, prohibitions and bans. In actual practice, nobody checks the list to see what he can or cannot do. People help and protect each other based on what is required in the given situation. The same principle applies to parents. They listen to their children’s needs and respond to them. The legal term ‘duty of care’ links up with this idea. But, is it also possible to combat cyber crime with duties of care? Research will have to establish that.*

ZORGPLICHTEN EN CYBERCRIME

DUTIES OF CARE AND CYBER CRIME

Het voordeel van een zorgplicht is dat burgers zelf moeten bedenken wat goede zorg is, in de gegeven situatie. Dat hoeft de overheid niet voor hen te bedenken. Door het algemeen te houden en niet strak vast te leggen, zullen zorgplichten daardoor vanzelf meebewegen met de tijd en de techniek. Nadeel is wel, dat via deze algemene aanpak niet voor alles gezorgd kan worden. Daarom is het goed dat de overheid in beperkte mate zorgplichten oplegt aan burgers, om zo de maatschappelijke werkelijkheid te reguleren.

Vertrouwen

Het is verleidelijk om zorgplichten in te zetten tegen nieuwe problemen en ze aan leveranciers van bijvoorbeeld IT-diensten op te leggen. Maar dat is lastiger dan het lijkt. Een zorgplicht veronderstelt namelijk dat al bekend is wat goede zorg is. Als het echter om problemen gaat in nieuwe situaties, is dat niet het geval. Het opleggen van zorgplichten blijft dan een lege huls. In dit kader is het dan ook zaak zorgplichten niet te streng te handhaven. Het gaat immers uit van de eigen verantwoordelijkheid van de ‘zorgverlener’ en vertrouwen in zijn eigen oordeel. Te veel wantrouwen vernietigt de voordelen van zorgplichten en leidt tot het strak reguleren en handhaven van de zorgplicht. Hier is de samenleving niet bij gebaat. Daarom is het nuttig om de werking van zorgplichten te onderzoeken. Het helpt om te begrijpen hoe de samenleving zichzelf kan reguleren.

KUN JE MET ZORGPLICHTEN CYBERCRIME BESTRIJDEN?

IS IT POSSIBLE TO COMBAT CYBER CRIME WITH DUTIES OF CARE?

The advantage of a duty of care (if taken broadly, including contractual diligence) is that citizens have to think about what proper care is in a particular situation. They do not need the government to think for them. By keeping it general and not being too strict about it, duties of care will adapt themselves to the time and technology. A disadvantage, however, is this general approach does not cover all the bases. It is a good thing that the government imposes duties of care on citizens – albeit limitedly - in order to regulate realities of society.

Trust

It is tempting to use duties of care to fight new problems and to impose them on, for instance, suppliers of IT services. But this is more difficult than it seems. A duty of care presupposes that people know what proper care is. When it comes to problems in new situations, this is not always the case. Imposing a duty of care thus remains an empty shell. In this context, it is important not to be too strict with upholding the duties of care, because the duty of care is based on the personal responsibility of the person ‘caring’ and on the confidence in his judgement. Too much distrust cancels out the advantages of duties of care and results in too strict regulating and upholding. This would have an adverse effect on society. Therefore, it is useful to investigate the workings of the duties of care, as it helps to gain insight in how society can regulate itself.

Nederland, Eindhoven, 15-02-14
Hackers proberen in het systeem van gemeente Eindhoven te hacken in het stadhuis.

The Netherlands, Eindhoven, 15-02-14
Hackers trying to hack the system of the municipality of Eindhoven.

Hollandse Hoogte

DE JURIDISCHE REGELS DIE ISP´S NU AANMOEDIGEN TOT PASSIVITEIT, MOETEN WORDEN AANGEPAST.

THE LEGAL FRAMEWORK THAT IS CURRENTLY HOLDING BACK ISPs SHOULD BE ADJUSTED

Onderzoek

Op dit moment loopt er een onderzoek naar de mogelijkheid om cybercrime te bestrijden met behulp van zorgplichten voor partijen die invloed hebben op dit onderwerp. De voorlopige resultaten zien er als volgt uit:

- De belangrijkste partijen zijn Internet Service Providers (ISP's) en softwareproducenten, naast bedrijven en burgers. Van burgers kan niet te veel worden verwacht, deels vanwege fundamentele rechten en deels om praktische redenen zoals gebrek aan expertise.
- ISP's zijn al actief tegen cybercrime. Zij hebben er immers zelf last van. Zij zijn echter niet verplicht het internet te bewaken. Bovendien ontmoedigen principes als netneutraliteit, privacybescherming en het recht op internettoegang hen actief te controleren op criminele activiteiten.
- Softwareproducenten kunnen meer doen om software veilig en zorgvuldig te ontwikkelen, maar de markt dwingt hen om software te snel vrij te geven.
- Bedrijven hebben een zorgplicht voor hun klanten als het gaat om beschikbaarheid van dienstverlening en vertrouwelijkheid van klantgegevens. Zij treffen doorgaans al vrij veel maatregelen, al zou misschien meer mogelijk zijn.
- Er zijn weinig goede en effectieve standaarden. Door de snelle ontwikkelingen is het lastig vast te stellen wat een goede handelswijze is.

Stimuleren

Om zorgplichten te stimuleren in het kader van cybercrimebestrijding, lijken diverse maatregelen zinvol. De juridische regels die ISP's nu aanmoedigen tot passiviteit, moeten worden aangepast. Zo kan ruimte gecreëerd worden voor ISP's om cybercrime te voorkomen en op te sporen. Voor de belangrijkste standaardsoftware zouden extra veiligheidsprikkels moeten komen. Denk aan een vorm van productaansprakelijkheid, een verplichting om vergoedingen te geven voor onderzoekers die kwetsbaarheden ontdekken en een verplichting om kwetsbaarheden te melden. Daarmee zou een aanzet kunnen worden gegeven voor praktijken die de cyberveiligheid bevorderen, zonder dat de overheid deze hoeft in te vullen.

Research

There currently is an investigation into the option of fighting cyber crime with the aid of duties of care for parties who influence this area. The preliminary results are as follows:

- The most important parties are Internet Service Providers (ISPs) and software manufacturers, followed by companies and citizens. One cannot expect too much from citizens, in view of their fundamental rights and partially for practical reasons, such as lack of expertise.
- ISPs are already fighting cyber crime, as they suffer the most from it. However, they do not have an obligation to 'defend' the internet. Moreover, principles such as net neutrality, privacy protection and the right to internet access actively discourage them to check for criminal activity.
- Software manufacturers could do more to develop safe and precise software products, but the market is forcing them to release software quickly.
- Companies have a duty of care towards their customers when it comes to availability of services and confidentiality of customer data. They generally take a fair amount of measures, although they could do more perhaps.
- There are not a lot of good and effective standards. Due to the fast developments, it is difficult to determine what good practice is.

Promote

To promote duty of care in the context of combating cyber crime, various measures seem to be useful. For example, the legal framework that is currently holding back ISPs should be adjusted to create room for ISPs to prevent and detect cyber crime. Extra security incentives should be created for the most important standard software products. This could include product liability, an obligation to grant researchers a fee for detecting vulnerabilities and an obligation to report vulnerabilities. This could be a prelude to practices that promote cyber security without the government needing to step in.

PIETER SCHOEHUIJS

Chief Information Officer AkzoNobel
Board member of the CIO Platform

EEN GEZAMENLIJKE AGENDA VOOR CYBERSECURITY

A JOINT AGENDA FOR CYBER SECURITY

‘In 2014 werden we in Nederland wakker geschud door relatief veel cyberaanvallen. Ze worden steeds geavanceerder en nemen toe in hevigheid en reikwijdte. Afgelopen jaar hadden we in onze industrie bijvoorbeeld een Stuxnetaanval die het specifiek had gemunt op onze procescontrolesystemen in de fabriek. Aan de andere kant willen medewerkers overal kunnen werken en net zo gemakkelijk als thuis gebruik maken van sociale media en meerdere mobiele apparaten. Die werelden staan op gespannen voet met elkaar.

Voorkomen cyberaanvallen

Veel apparaten zijn verbonden in een fabrieksnetwerk, dat weer is gekoppeld aan een kantoornetwerk en het internet. Soms zijn apparaten ook direct gekoppeld aan het internet, bijvoorbeeld om op afstand storingen uit te lezen. Deze toepassingen dienen het gemak, maar zijn ook een punt van zorg. Zonder de juiste maatregelen zouden hackers de controle over kunnen nemen, processen verstoren of gevoelige bedrijfsgegevens verzamelen.

Grote bedrijven beschikken over verschillende ICT-beveiligingslagen. Maar er zijn nog maar weinig bedrijven die een samenhangende strategie hebben die systematisch in beeld brengt welke data en infrastructuur kwetsbaar is voor cyberaanvallen. Het is ook lastig om een sluitend beeld te hebben, zeker als je wereldwijd werkt. AkzoNobel heeft bijvoorbeeld 1.000 locaties, 4.500 servers en 1.500 applicaties.

Divers gezelschap

Het CIO Platform Nederland is een onafhankelijke vereniging van CIO’s en IT-directeuren van grote private en publieke organisaties in Nederland. Ik vind dat cybersecurity nog hoger op de agenda van de Nederlandse boardrooms moet komen. We hebben technologisch nog van alles te doen. Maar ook awareness bij medewerkers is belangrijk. En we moeten zorgen voor duidelijke en veilige standaardprocedures waar mensen zich ook aan houden. Bij alle drie deze aspecten is er de komende jaren nog verbetering mogelijk.

De Cyber Security Raad speelt hierin een mooie rol. Het is een heel divers gezelschap. Met vereende kracht agenderen we prioriteiten bij de minister. Deze prioriteiten delen we met onze achterbannen. En met die gezamenlijke agenda helpen we de cybersecurity In Nederland weer verder vooruit.’

‘In 2014 we were rudely awakened in the Netherlands by a relatively large number of cyber attacks. These are becoming increasingly more advanced and they are growing in their intensity and scope. Last year, for example, in our industry we suffered a Stuxnet attack, which was aimed specifically at our process control systems at factories. On the other hand, employees want to be able to carry out their work in a variety of places and make use of social media and other mobile machines, just as they do at home. Those worlds are at odds with each other.

Preventing cyber attacks

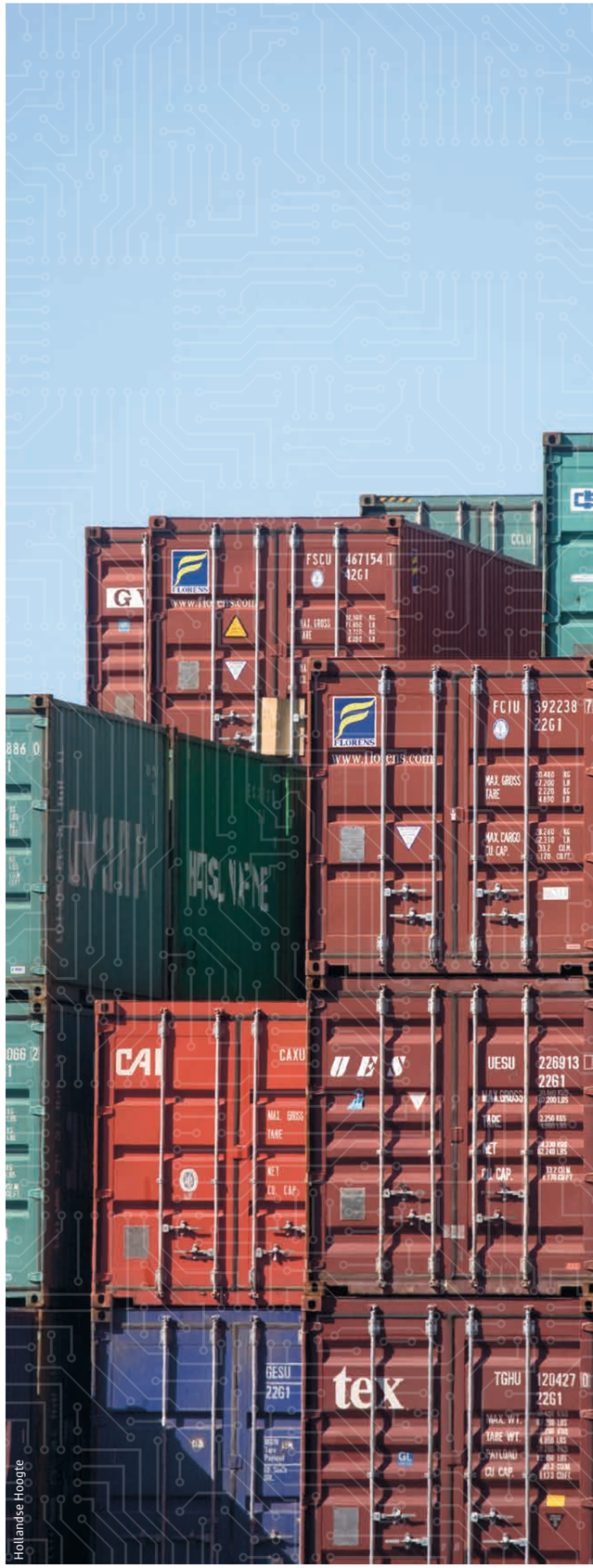
Many machines are connected to a factory network, which itself is coupled to an office network and the internet. Machines are also sometimes coupled to the internet, for example for the purpose of checking malfunctions remotely. These applications serve our convenience, but they are also a cause for concern. Without having the correct measures in place, hackers could take over control, disrupt processes or gather sensitive business data.

Large businesses have a variety of IT security levels available to them. But there are very few businesses that have a cohesive strategy, which systematically draws attention to which data and infrastructure may be most sensitive to cyber attacks. It is, of course, very difficult to put together a clear picture, particularly for businesses working globally. AkzoNobel, for example, has over 1,000 locations, 4,500 servers and 1,500 applications.

Diverse group

The CIO Platform Netherlands is an independent association of CIOs and IT directors of large private and public organisations in the Netherlands. I believe that cyber security should be placed higher on the agenda of the Dutch boardrooms. Technologically speaking, there is still a great deal to be done. However, the awareness of employees is most important. And we also need to provide clear and safe standard procedures, which people can continually refer to. In relation to each of these three aspects, it is possible to achieve improvements over the next few years.

The Cyber Security Council plays a useful role in this. It comprises a very wide variety of participants. With a united effort we can put priorities to the minister. We will share these priorities with our employees. And with that joint agenda we will be able to help move cyber security in the Netherlands further forward.’



Hollandse Hoogte

Computers zitten vol met fouten en lekken, vindt hoogleraar Bart Jacobs. Wat gaan we daar aan doen? Er is geen makkelijke oplossing, maar: ‘De overheid mag best wat assertiever zijn.’ *Computers are full of mistakes and leaks, thinks Professor Bart Jacobs. What are we going to do about that? There is no simple solution, but: ‘The government could certainly be more assertive about the matter.’*

FOLLOW THE DATA


Arvet Bleumer

BART JACOBS

Professor of Software Security and Correctness
Radboud University Nijmegen

Jacobs: ‘We hebben allerlei problemen op ICT-gebied. Wat doen we daar aan: de gebruiker op de vingers tikken of betere systemen bouwen? ICT-bedrijven denken het eerste, ik niet. De overheid is niet streng genoeg voor de ICT-sector. Wekelijks lezen we in de krant over cybersecurity-incidenten. Dan kun je niet blijven zeggen: de mensen zijn onvoorzichtig geweest. Het is op zijn minst een wisselwerking. We maken websites waarin staat dat jij geen domme dingen moet doen. Maar dat vind ik hetzelfde als vertellen hoe je veilig kunt rijden met een kapotte auto.’

Digitale tv’s en slimme meters

‘Ik maak me zorgen over de schuivende machtsverhoudingen’, vervolgt Jacobs. ‘Door de verdergaande digitalisering verliest de burger steeds meer autonomie. Meer en meer partijen verzamelen gegevens over ons. Zelfs in ons huis, waar verschillende apparaten digitaal worden aangestuurd. Onze digitale tv’s slaan op wat we kijken en de slimme meters zien wanneer we thuis zijn. Ik mis een duidelijke visie over wie onder welke omstandigheden bij die gegevens zou moeten kunnen.’

Jacobs: ‘Om de gezagsverhoudingen in de samenleving te begrijpen, zeiden we vroeger: “follow the money.” Nu is dat geworden: “follow the data.” Bij elk wetsvoorstel moeten we niet alleen kijken waar het geld aan wordt uitgegeven, maar ook waar de gegevens naartoe gaan. Dat besef is er nog te weinig.’

De discussie scherp houden

Jacobs is verbonden aan de Radboud Universiteit Nijmegen. Hier vindt de enige bacheloropleiding cybersecurity van Nederland plaats. De masteropleiding bestaat al langer en leidt studenten op tot het hoogste niveau, master in de informatica en cybersecurity. Jacobs: ‘Als wetenschapper breng ik in de Raad vooral kennis in over nieuwe ontwikkelingen. Het is voor mij ook interessant om te horen hoe de overheid en het bedrijfsleven tegen dingen aankijken. Daarnaast kijken wetenschappers vaak net wat anders tegen zaken aan. Mijn rol is dan ook om de discussie scherp te houden. Om af en toe te vragen: ‘Is dat nu wel zo?’

‘Het beleid over responsible disclosure and repair is één van de successen waar de Cyber Security Raad duidelijk een stimulerende rol in heeft gespeeld. Op dit onderwerp is vrij snel beleid gekomen. Een ander onderwerp waar we in de Raad over praten en dat steeds meer weerklank vindt, is zorgplicht voor ICT-bedrijven. Veel mensen weten weinig van ICT, de fabrikanten juist heel veel. Er is een enorme kennisasymmetrie. Bedrijven moeten zich dus verantwoordelijk gedragen en net als bijvoorbeeld banken een zorgplicht krijgen. Hier zou de overheid een stevige rol in kunnen spelen.’

Incidenten koesteren

Dat reguleren mogelijk is, bewijzen de regels voor netneutraliteit, vindt Jacobs. Aanbieders van internet mogen sinds 2013 diensten of toepassingen van concurrenten niet zomaar blokkeren of vertragen. Jacobs: ‘Nederland loopt op dit punt wereldwijd voorop. Ook het Europese parlement heeft netneutraliteit omarmd. Telecombedrijven waren natuurlijk tegen deze regels. Ze mogen bijvoorbeeld niet Whatsapp blokkeren om het sms-verkeer te stimuleren. Het is belangrijk om mensen te beschermen tegen commerciële uitbuiting.’

‘De uitdaging voor de komende jaren is ICT-producten minder complex te maken. Dan moet je wel dingen gescheiden houden. Als je wilt dat mensen beveiligd bellen, dan moet je niet op die telefoon gaan Skypen of Facebooken. Maar veel mensen hebben daar geen zin in. Daarom moet je cyberincidenten koesteren, want pas als het goed mis gaat kun je zaken echt veranderen.’

Jacobs: ‘We have all sorts of problems in the area of IT. What do we do about this: punish the user or build better systems? IT businesses believe in the former option, but I don’t. The government is not strict enough with the IT sector. Every week we read about cyber security incidents in the press. You can’t keep on saying: people are behaving carelessly. At the very least, it’s a matter of interaction. We make websites in which it states that you shouldn’t do anything stupid. But I think it’s the same thing as telling someone how to drive carefully in a faulty car.’

Digital TVs and clever meters

‘I’m concerned about the shifting balance of powers’, Jacobs continues. ‘Due to the increasing digitalisation, the public are losing more and more autonomy. Ever-increasing numbers of parties gather information about us. Even in our own homes, where a variety of different machines are operated digitally. Our digital TVs record what we watch and the clever meters see when we are home. I miss a clear vision about who should have access to that data, and under what circumstances.’

Jacobs: ‘In order to understand the authority relationships in society, we used to say: follow the money. That has now changed to: follow the data. In the case of every legislative proposal we should not only look at where the money is spent, but also where the data is distributed. That perception is all too often lacking.’

Keeping the discussion relevant

Jacobs works at Radboud University in Nijmegen. This university provides the only bachelor’s degree in cyber security in the Netherlands. The master’s degree course has existed for longer and it provides education to students at the highest level, master in information sciences and cyber security. Jacobs: ‘As a scientist, I mainly provide knowledge to the Council concerning new developments. I also find it interesting to hear how the government and the business community view matters. Moreover, scientists tend to look at matters in a different light. My role is therefore to keep the discussion relevant. To pose the question every now and again: ‘Is that really the case?’

‘The policy concerning responsible disclosure and repair is one of the successes in which the Cyber Security Council has played a stimulating role. Policy was relatively quickly developed on this subject. Another subject which we discuss in the Council, and which receives an increasing response, is the duty of care for IT companies. There are so many people who know little about IT, but the manufacturers know a great deal. There is an enormous asymmetry in the knowledge. Companies must therefore behave responsibly and, just like the banks for example, be issued with a duty of care. The government could play a strong role in relation to that.’

Cherish incidents

The rules for net neutrality prove that regulation is possible, thinks Jacobs. Since 2013, internet suppliers are not permitted to block or delay services or applications of their competitors without reason. Jacobs: ‘On this point, the Netherlands is ahead in worldwide terms. The European Parliament has also embraced net neutrality. Telecom businesses were, of course, against these rules. They are not permitted to block WhatsApp, for example, in order to stimulate text messaging. It is important to protect people against commercial exploitation.’

‘The challenge for the next few years is to make IT products less complex. You then need to keep things separate. If you want people to make telephone calls in a secure environment, then you cannot allow that telephone also to be used for Skype or Facebook. But many people are not interested in that. Therefore you must cherish any cyber incidents, since you can only change things once serious damage has been done.’

‘CYBER RAAKT ALLE WERK-PROCESSEN VAN DE POLITIE’

‘CYBER AFFECTS ALL THE WORK PROCESSES OF THE POLICE’

Josje Deekens

‘Alle onderwerpen in de Cyber Security Raad raken op een of andere manier de politietaak. Of het nu gaat om cybercrime, technologische ontwikkelingen of mogelijke veiligheidsmaatregelen: de politie heeft er een rol in’, vertelt Jannine van den Berg. *‘All the subjects in the Cyber Security Council affect the police tasks in one way or another. Whether this involves cyber crime, technological developments or possible security measures: the police play a role’, says Jannine van den Berg.*

Van den Berg is als directeur Operatiën van de Nationale Politie lid van de Cyber Security Raad. Vanwege de vorming van de Nationale Politie wordt haar plaats tijdelijk waargenomen door Chief Information Officer Dick Heerschop.

Nieuwe vormen van criminaliteit

Heerschop: ‘Het internet biedt veel kansen, maar elke ontwikkeling heeft ook een schaduwzijde. Er ontstaan bijvoorbeeld nieuwe vormen van oplichting. De oude criminaliteit in een nieuw jasje komt veel voor, dus het inbreken in je computer in plaats van in je huis. Er zijn ook vormen van criminaliteit die door het internet een enorme vlucht hebben genomen, denk aan kinderporno. En we kennen natuurlijk criminaliteit waarbij het internet zelf het doelwit is, zoals DDoS-aanvallen. Deze ontwikkelingen leggen een druk op de innovatiekracht van de politie. We moeten voortdurend voorop lopen en dat lukt ons gelukkig goed. Een gerenommeerd cybersecurity-bedrijf heeft ons Team High Tech Crime genoemd als een van de beste teams ter wereld.’

Internet helpt ook

‘Cyber raakt al onze werkprocessen,’ vervolgt Van den Berg, ‘niet alleen de opsporing, maar ook de ordehandhaving, inlichtingen en dienstverlening. Met internet kunnen we bijvoorbeeld de toevoer van mensen reguleren, zoals we tijdens de kroning deden via een speciale app. Maar door internet kunnen we ook betere informatie leveren aan onze mensen op straat. Als een agent naar een adres gaat in verband met huiselijk geweld, kijken we direct in alle systemen en openbare bronnen. Zo weten agenten beter wat ze daar aantreffen. Ook verzamelen we data met automatische nummerplaatherkenning waardoor we snel weten waar een overvaller heen vlucht.’

Iedereen digitaal vaardig

Van den Berg: ‘Het internet helpt ons dus ook in ons werk. We willen daarom dat iedere politieman of -vrouw een goede basiskennis heeft van de digitale wereld. Niet elke wijkagent hoeft te twitteren, maar je moet wel weten wat je er aan hebt. En als je als rechercheur een huiszoeking doet, dan moet je weten hoe je omgaat met de apparatuur die je aantreft. Niet klakkeloos de stekker uit de computer trekken en hem onder je arm meenemen.’

Dick Heerschop pleit voor meer aandacht hiervoor in het onderwijs. ‘Kinderen die nu opgroeien, moeten voldoende digitaal vaardig zijn om hun rol in de samenleving te kunnen oppakken. Of ze nu bij de bank gaan werken of bij de politie. Daar is nog een hele slag te maken. Eén van de speerpunten van de Cyber Security Raad is dan ook om de verbinding met het onderwijs te versterken. De politie geeft zelf ook gastlessen aan kinderen over de keerzijde van sociale media. Want naast de opsporing vinden we ook de preventie van cybercrime erg belangrijk.’

Cyber is grenzeloos

Van den Berg kijkt uit naar de Global Conference on CyberSpace 2015. ‘Het elektronisch domein is grenzeloos en daarom werken we internationaal al veel samen. We werken samen met andere landen via internationale rechtshulpverzoeken, maar ook met het European Cybercrime Centre van Europol.’ Van den Berg: ‘Het is belangrijk dat we de kennis en kunde van ander landen kennen. Wij hebben een Cyber Security Raad, maar hoe doen ze het elders? Wereldwijd ontwikkelen landen zich snel op het cyberdomein, daarom zijn dit soort internationale bijeenkomsten zo waardevol.’

As director of Operations of the National Police Force, Van den Berg is a member of the Cyber Security Council. Due to the forming of the National Police Force, her place is temporarily represented by Chief Information Officer Dick Heerschop.

New forms of criminality

Heerschop: ‘The internet offers huge opportunities, but every development also has a darker side. For example, we see new forms of fraud. The old crimes often present themselves in a new disguise, hence the break-in of your computer instead of your home. There are other forms of crime that have increased enormously due to the internet, for example child pornography. And of course we see crime whereby the internet itself is a target, such as with the DDoS attacks. These developments put pressure on the innovative power of the police. We need to keep one step ahead all the time and we are succeeding in doing that. A reputable cyber security company called our Team High Tech Crime one of the best teams in the world.’

Internet also helps

‘Cyber affects all the work processes of the police’, Van den Berg continues. ‘Not only in the detection, but also in maintaining public order, providing information and services. Using the internet we can regulate the flow of people, for example, which we did during the recent coronation ceremony by using a special app. But we can also provide better information over the internet to our forces on the streets. If an officer travels to an address in connection with domestic violence, then we immediately check in all our systems and public sources. This allows officers to know better what they are likely to find there. We gather data as well using automatic number plate recognition, which allows us to find out quickly where a robber has fled to.’

Everyone has digital skills

Van den Berg: ‘Therefore the internet helps us in our work. This means that we want every policeman or policewoman to have a good basic knowledge of the digital world. Not every community police officer has to use Twitter, but you need to be aware of its uses. And if as detective you carry out a search in someone’s home, then you need to know how to handle the machines that you find there. You can’t necessarily just pull out the plug of the computer and take it away.’

Dick Heerschop argues the case for greater attention to be given to this in the education system. ‘Children growing up in this age must be sufficiently digitally skilled in order to face the roles they play in our society. Whether they go to work in a bank or by the police. This requires much more work. One of the key focus areas of the Cyber Security Council is therefore also to strengthen the connection with the education system. The police themselves give guest lessons to children about the drawbacks of social media. Because, besides detection, we also believe that the prevention of cyber crime is extremely important.’

Cyber is without borders

Van den Berg is looking forward to the Global Conference on Cyberspace 2015. ‘The electronic domain is without borders and for this reason we are already working a great deal together internationally. We work together with other countries via international requests for assistance, but also using Europol’s European Cybercrime Centre.’ Van den Berg: ‘It is important that we are up-to-date with the knowledge and skills of other countries. We have a Cyber Security Council, but what do they do elsewhere? Countries all around the world are quickly developing themselves in the cyber domain, which is why these types of international meetings are so valuable.’

By **Elly van den Heuvel**,
Secretary of the Cyber Security Council (CSR)

INTERNATIONAL COOPERATION BETWEEN CYBER SECURITY COUNCILS

The Dutch Cyber Security Council (Nederlandse Cyber Security Raad, CSR) has a strong public-private character. Strategic problems in the cyber domain are approached from a multidisciplinary angle. It does not concern threats alone, but also social and economic opportunities. The CSR is looking explicitly at cooperation with councils in other countries and welcomes the establishment of more of these councils. Hence a brief look into how the CSR is organised in the Netherlands.

The Dutch CSR is a national and strategic advisory body. The CSR was formed by ministerial order and advises the government. The CSR also advises organisations in, for example, the vital sectors. The Council is formed from highly-placed representatives in scientific, public and private organisations: The private members represent their supporters, such as a trade association. Problems are approached from various angles and the various interests are handled according to priority in the advice.

Balanced composition

To be able to provide independent and well-considered advice, the Dutch CSR is put together with a balanced composition. Representatives of public and private parties each hold seven seats. Scientific institutions hold four seats. The council has two co-chairmen: the government and private sector alternate with each other every meeting.

Clear terms of reference

Cyber security is a field in which many parties are active. The Dutch CSR therefore has a clear position and terms of reference:

- providing solicited and unsolicited advice on cyber security to the government and private parties,
- advising the government on the implementation and development of the National Cyber Security Strategy II,
- contributing to research in the scope of the Dutch Cyber Security Research Agenda,
- deploying CSR members during large-scale cyber incidents.

In addition, the members hold personal discussions at boardroom level in order to get cyber security on the agenda at strategic level.

Strategic level

The Council is forward-looking and develops a strategic vision of new technological developments. What lies ahead of us in the medium and long term? And what does this mean for the future approach to cyber security and cyber crime?

Would you like more information? Then please contact the Cyber Security Council at e.c.van.den.heuvel@nctv.minvenj.nl.

Colofon ◦ *Colophon*
Opdrachtgever ◦ ***Commissioning party***: Cyber Security Raad Nederland, *Dutch Cyber Security Council*
Hoofdredactie ◦ ***Chief editor***: Elly van den Heuvel (secretaris, *secretary*)
Inhoudelijk adviseur ◦ ***Content advisor***: Eline Attema
Concept en procesbegeleiding ◦ ***Concept and process management***: Martin Bobeldijk (Turnaround Communicatie)
Tekst en grafische vormgeving ◦ ***Text and graphic design***: Tappan Communicatie
Drukwerk ◦ ***Printing***: Impressed

CSR Cyber Security Council Cyber Security Raad