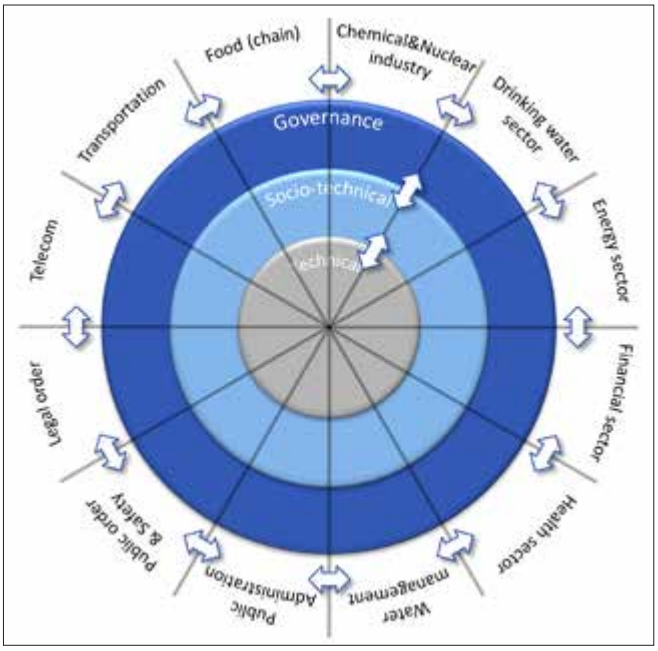
Wat maakt cyber security anders dan informatiebeveiliging?

De termen “informatiebeveiliging” en “cyber security” worden vaak door elkaar gebruikt soms met dezelfde, soms met een afwijkende betekenis. Velen spreken vandaag de dag ook over cyberspace, bijvoorbeeld als een nieuw (door de mens gecreëerd) vijfde domein naast de bestaande domeinen land, water, lucht en ruimte. Een en ander roept de vraag op of informatiebeveiliging en cyber security (wel of niet) fundamenteel van elkaar verschillen. Geconfronteerd met de uitdaging om nieuw multidisciplinair onderzoek & onderwijs rond cyber security te ontwikkelen, ontstond de noodzaak om orde op zaken te stellen en de begrippen helder ten opzichte van elkaar te positioneren. Dit heeft geleid tot een nieuwe conceptualisatie rond de begrippen cyberspace en cyber security. Informatiebeveiliging is in deze visie onderdeel van het bredere begrip van cyber security. De eerste ervaringen rond het gebruik van dit nieuwe begrippenkader zijn zeer positief.

Prof. dr. ir. Jan van den Berg
Hoogleraar Cyber Security TU Delft, wetenschappelijk directeur Cyber Security Academy (j.vandenberg@tudelft.nl)

Informatiebeveiliging gaat over de maatregelen en procedures om beschikbaarheid, exclusiviteit en integriteit van informatievoorziening te garanderen en in het bijzonder om de continuïteit van de informatie en informatievoorziening te waarborgen en de gevolgen van incidenten tot een acceptabel niveau te beperken. Hoewel *cyber security* vaak met een vergelijkbare definitie wordt omschreven zoals het “het vrij zijn van gevaar of schade veroorzaakt door verstoring of uitval van ICT of door misbruik van ICT” bijvoorbeeld door “beperking van de beschikbaarheid en betrouwbaarheid van de ICT” (*Cyber Security Beeld Nederland 4*), wordt de term cyber security ook gebruikt als term voor het *beveiligen van cyberspace*. *Cyberspace* werd als eerste door de militairen aangeduid als het *vijfde domein*, simpelweg omdat er behoefte bleek te bestaan aan een nieuw type soldaten (naast soldaten actief op land, ter zee, in de lucht en de ruimte).

Inmiddels hebben we ons, bij vrijwel alles wat we doen (werken, reizen, vrijetijdsbesteding), sterk afhankelijk gemaakt van ICT en kunnen we spreken van *cyberactiviteiten*. Cyberactiviteiten zijn alle activiteiten die via ICT mogelijk gemaakt worden en dat zijn er een hoop. Naast het uitwisselen van data en informatie (via diensten als email, WhatsApp, Twitter, Skype, Spotify, televisie, enz.) betreft dit zoekfunctionaliteiten (zoals via diensten als Google, 9292.nl, buienradar.nl, KNMI.nl), gaat het om transacties (op basis van o.a. e-business), gaat het ook om het (op afstand) besturen van vitale infrastructuren (zoals rond watervoorziening, gas- en elektriciteitsproductie & -distributie), vinden we onze nieuwe vrienden via Internet (zoals via Facebook, 2nd love), voeren we actie en maken propaganda op Internet (bv Wikileaks), vindt er diefstal en fraude plaats (zoals in het dark web) en voeren we zelfs cyberoorlogen (met behulp van drones en logische cyberwapens zoals Stuxnet). *Cyberspace is de wereld van al deze cyberactiviteiten* en het zijn deze activiteiten die besturing of, met een Engelse term, governance behoeven.



Figuur 1 *Conceptualisatie cyberspace in lagen (ringen) en (cyber) sub-domeinen.*

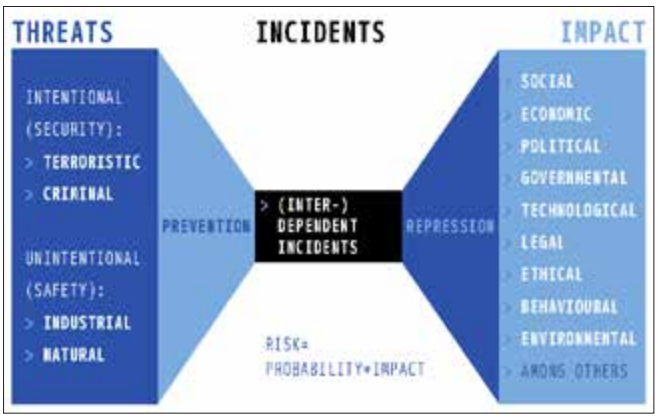
Bovenstaande analyse geeft aanleiding tot een 3-*laags cyberspace model:*

1. de *technische laag maakt* cyberactiviteiten mogelijk – is de onderste laag;
2. de *laag van cyberactiviteiten* waar techniek en mens met elkaar interacteren – is de middelste *socio-technische laag;*
3. de *governance laag* van waaruit de twee andere lagen aangestuurd kunnen en moeten worden – is de bovenste laag.

Het grote voordeel van de uitsplitsing in laag 1 en 2 is dat we onderscheid maken tussen de ICT-laag die faciliteert en de socio-technische laag die de cyberactiviteiten expliciet maakt: cyberactiviteiten zijn activiteiten in de context van bepaalde ICT, deze geven betekenis (terwijl ICT *an sich*, zonder context, eigenlijk betrekkelijk betekenisloos is). Daarmee worden de *key assets van analyse* ook de cyberactiviteiten en niet meer de (betrekkelijk abstracte en betekenisloze) informatie en ICT.
Door de lagen als ringen te representeren ontstaat een *ringenmodel van cyberspace* dat op natuurlijke wijze kan worden opgesplitst in *cyber sub-domeinen*: in ieder cyber sub-domein vinden domein-specifieke cyberactiviteiten plaats. Een visualisatie van deze conceptualisatie van cyberspace staat in figuur 1.

CYBER SECURITY UITDAGINGEN

In de vroegere dagen van informatiebeveiliging was de focus consequent op de begrippen beschikbaarheid, exclusiviteit en integriteit van de informatievoorziening. Deze begrippen zijn nog steeds van toepassing, maar, binnen de nieuwe conceptualisatie, alleen in de technische laag (!).
Kijkende naar huidige *best practices* in informatiebeveiliging (zoals de ISO-IEC27000-series), dan zijn een aantal business georiënteerde onderwerpen zoals *cyberspace assets*, *supplier relationships*, *business continuity management* en *compliance* inmiddels geadopteerd. Dit kan worden gezien als een eerste stap richting ons model, namelijk naar de lagen 2 en 3 ervan. *Business continuity* bijvoorbeeld betreft, in een breder perspectief, *continuïteit van de cyberactiviteiten*, hetgeen een veiligheidsaspect van de nieuwe *key assets* betreft. En *compliance* is typisch een onderwerp van de governancelaag dat de cyberactiviteiten beschouwt in het kader van wet- en regelgeving.
De gegeven analyse leidt op een natuurlijke wijze tot het begrip *Cyber Risico Management*. Cyberspace-actoren (van eindgebruikers tot op zichzelf staande organisatie tot netwerkorganisaties, organisaties die samenwerken in een supply chain, kritieke infrastructuren en landen) lopen allemaal zekere *cyberrisico's* omdat, onder invloed van talloze bedreigingen (inclusief de uitval van ICT), hun cyberactiviteiten gevaar lopen. Dit laat nogmaals zien dat, binnen de nieuwe conceptualisatie, de cybercontext waarin de ICT wordt gebruikt centraal komt te staan. Gebruikmakend van het zogeheten "bowtie-model" gaat het bij Cyber Risico Management in essentie om:



Figuur 2 Cyber Risico Management op basis van het "bowtiemodel".

a. het *identificeren en schatten van cyberrisico's* (dat zijn risico's gerelateerd aan mogelijk optredende "cyber activity breaches");
b. het vaststellen van *acceptabele cyberrisiconiveaus* (een politieke beslissing);
c. het ontwerpen en implementeren van een *gebalanceerde verzameling van preventieve en correctieve maatregelen* ten einde de vastgestelde cyberrisico's tot de gewenste proporties terug te brengen.

Een en ander is gevisualiseerd in figuur 2.

SLOTOPMERKINGEN

De bovenstaande conceptualisatie van cyberspace en cybersecurity verbreedt het onderwerp van studie op een natuurlijke wijze van een (mogelijk) puur technische naar een socio-technische met als focus cyberactiviteiten (die iedereen, inclusief de board, begrijpt) én een governancelaag met als focus de aansturing van de complexe wereld van cyberspace. Dit maakt ook en *integrale benadering van cyber security* mogelijk waarin bijvoorbeeld risico's in al zijn dimensies geanalyseerd kunnen worden (zie de begrippen genoemd onder "IMPACT" in figuur 2) en allerlei principes van governance kunnen worden beschouwd in termen van effectiviteit en efficiency. Door cyber security per cyber sub-domein te beschouwen ontstaat een verdere verfijning van de analyse en aanpak hetgeen zeer gewenst is aangezien cyberrisico's sterk verschillend van karakter (kunnen) zijn.
Bovenstaande conceptualisatie is uitgangspunt geweest bij het ontwerp van het professional MSc programma Cyber Security dat momenteel op de Cyber Security Academy The Hague draait. De professionals die dit programma volgen, hebben het model omarmd en proberen er zo consequent mogelijk mee om te gaan. Gebleken is al dat het model vele discussies enorm verheldert. Wel is het zo dat, na jaren van training, het voor sommigen niet eenvoudig is om niet langer information security breaches (rond *CIA-disruptions*) als startpunt van denken te nemen maar inderdaad de cyberactiviteiten. Een en ander vraagt ook om een nieuw type van cyberrisicomanagement. Daarom biedt dit model ook talloze aanknopingspunten voor nieuw research. Maar al met al is dit startpunt van een nieuwe conceptualisatie van cybersecurity (dat informatiebeveiliging als onderdeel in zich draagt) veelbelovend omdat het een aantal concepten helder uit elkaar trekt. Meer details over dit onderwerp zijn te vinden in hieronder vermeld artikel, gepresenteerd tijdens het NAVO-symposium in Tallinn.

REFERENTIES

- http://nl.wikipedia.org/wiki/Informatiebeveiliging
- Cyber Security Beeld Nederland 4 (www.nctv.nl)
- ISO/IEC-27000-series http://en.wikipedia.org/wiki/ISO/IEC_27000-series
- D. Helbing, 'Globally networked risks and how to respond', *Nature*, 497 (May 2013), 51-59.
- https://www.csacademy.nl/en/education/master-s-programmes
- J. van den Berg, a.o, "On (the Emergence of) Cyber Security Science and its Challenges for Cyber Security Education", winner of the ***best paper award*** at the NATO STO/IST-122 symposium in Tallinn, October 13-14 2014.