INSPIRATION SERIES:

DE TOEKOMST VAN CYBERCRIMINALITEIT EN -TERRORISME

RICHARD
VAN HOOIJDONK
TRENDWATCHER & FUTURIST

Inspiratie sessies van trendwatcher & futurist

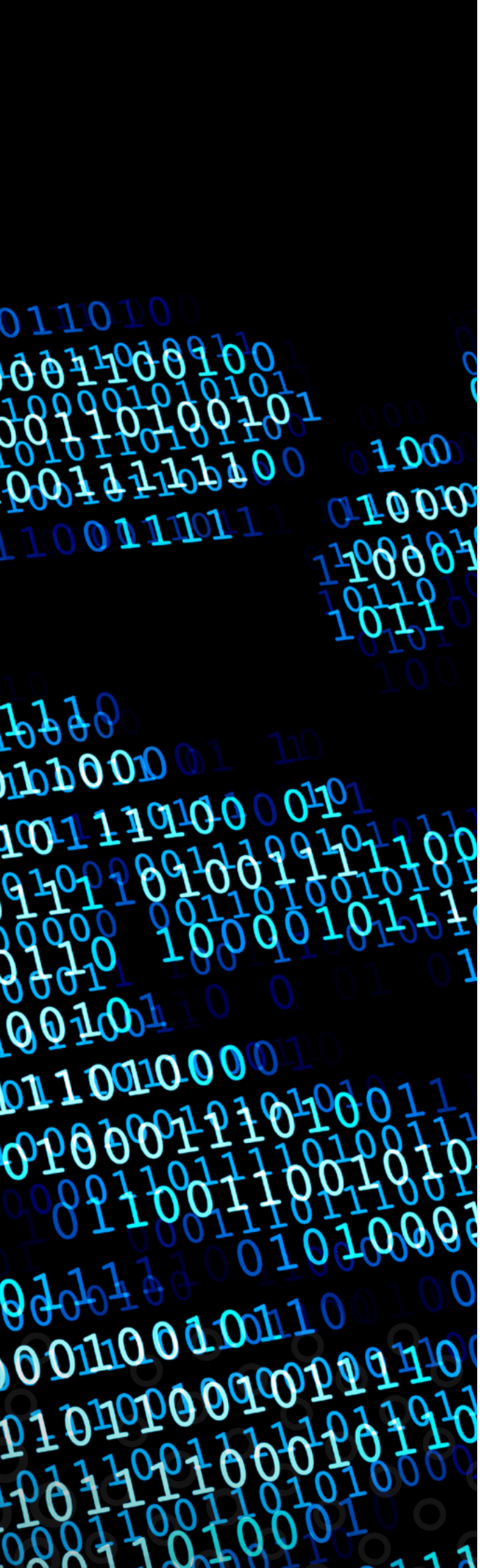
RICHARD VAN HOOIJDONK

Ben je klaar voor een reis naar de toekomst van jouw sector?

In onze inspiratiesessies zien we hoe de huidige technologische ontwikkelingen alles wat je dacht te weten over jouw (bedrijfs) leven veranderen. Boek een sessie en laten we de toekomst samen verkennen.

Ga voor meer informatie naar:
richardvanhooijdonk.com

INHOUD



INLEIDING

Technologie maakt ons leven gemakkelijker en het verbindt ons meer dan ooit. Zelfs onze slimme apparaten praten met elkaar. Zo kan Amazon's Echo bijvoorbeeld een pizza voor je bestellen en je slimme thermostaat kan zich aanpassen aan je aanwezigheid in een kamer. Deze innovaties worden gedreven door toegang tot het Internet of Things (IoT), maar naarmate dit onzichtbare web van communicatie groeit, worden we ook kwetsbaarder voor individuen met kwade bedoelingen.

Cybercriminaliteit en cyberterreur hebben nu al invloed op ons leven en de effecten ervan zijn breder dan je je kunt voorstellen. Van het hacken van ziekenhuizen tot het gijzelen van het elektriciteitsnet om stroomuitval te veroorzaken, hackers struinen het IoT af op zoek naar kwetsbaarheden. En het kan veel erger worden dan gestolen gegevens of verstoring van de infrastructuur: biotechnologie kan gemakkelijk worden gebruikt om massavernietigingswapens te maken en criminelen kunnen met 3D-printers hun eigen wapens printen.

De toekomst is weliswaar onzeker, maar de dreiging is reëel.

1.0

ONZE GEZONDHEID IN GEVAAR

"Cyberbeveiliging is iedereens taak. Nogmaals, waar je je echt op moet focussen is een veelzijdige aanpak waar je de gebruikers traint. Zij zijn de eerste verdedigingslinie."

- Dan Waddell, managing director van het International Information System Security Certification Consortium

Ook de gezondheidszorg verandert door technologie. Hoewel tech-ontwikkelingen ziekenhuizen en patiënten verschillende voordelen bieden, brengen ze ook risico's met zich mee. Onze cyberveiligheid komt bijvoorbeeld steeds vaker in gevaar – met potentieel dodelijke gevolgen.

Misschien ben je in het verleden al eens slachtoffer geweest van een smartphone- of computerhack. Maar dat is niks vergeleken bij wat er in de toekomst allemaal mogelijk is. Het menselijk lichaam is namelijk het nieuwste en kwetsbaarste doelwit voor hackers. Je kunt haast niet geloven dat het hacken van het lichaam mogelijk is, maar criminelen kunnen er potentieel veel geld mee verdienen en er zelfs mensen mee vermoorden. Een professionele atleet zou zijn rivaal bijvoorbeeld kunnen hacken om hem vlak voor een belangrijke race of wedstrijd uit te schakelen. Een cybercrimineel kan ook iemands gezondheid 'kidnappen' totdat hij of zij losgeld betaalt.

Medische implantaten kunnen makkelijker gehackt worden dan je denkt. Deze apparaten zijn vaak draadloos verbonden om ze op afstand te kunnen monitoren. Op deze manier kunnen medische professionals de behandeling gemakkelijk aanpassen zonder dat er invasieve ingrepen nodig zijn. Maar het feit dat ze op het IoT aangesloten zijn vormt een solide basis voor hackaanvallen. Volgens de Trend Micro-enquête worden ongeveer 36.000 medische hulpmiddelen in de VS zichtbaar gemaakt door de zoekmachine Shodan. Het is voor mensen met slechte bedoelingen makkelijk om misbruik te maken van deze connectiviteit. De informatie die via deze eenvoudig te krijgen medische apparaten verzameld kan worden, kan namelijk worden gebruikt voor belastingfraude of identiteitsdiefstal. Een groep studenten van de Universiteit van South Alabama heeft al aangetoond dat het hacken van dergelijke apparaten zelfs heel eenvoudig is. Ze konden toegang krijgen tot een pacemaker in een

dummy en de instellingen veranderen om effecten te veroorzaken die - naar alle waarschijnlijkheid - fataal zouden zijn voor een echte patiënt. Hoewel een van de toonaangevende fabrikanten van pacemakers, Medtronic, zegt dat de kans op hacking minimaal is, zijn de Amerikaanse autoriteiten zich terdege bewust van het potentiële risico. Het ministerie van Binnenlandse Veiligheid in Amerika is bezig de beveiliging van medische hulpmiddelen die gevoelig zijn voor dit soort cyberaanvallen te onderzoeken.

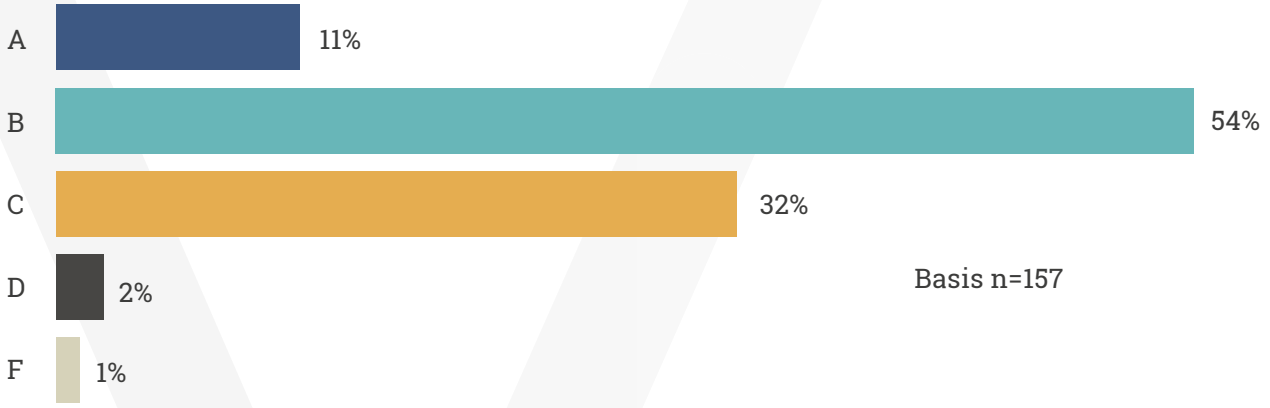
Net zo beangstigend als het idee dat een hacker jou via een medisch implantaat op afstand kan vermoorden, is het besef dat opkomende technologie aantoont dat zelfs je gedachten straks niet meer veilig zijn. Op de Enigma-conferentie introduceerde Tamara Bonaci, onderzoeker van de Universiteit van Washington, een experiment met een videogame waarbij "neurale responses op vertoonde subliminale beelden" verzameld werden. Tijdens het spel analyseerde Bonaci de subtiele elektrische signalen in de hersenen van proefpersonen als reactie op dingen die tijdens het spel onopvallend voorbij flitsten, zoals logo's van auto's en fastfoodrestaurants. In feite las Bonaci dus de gedachten van haar proefpersonen. Uit haar onderzoek blijkt echter dat deze methode ook gebruikt kan worden om gevoeligere informatie te achterhalen, zoals religieuze overtuigingen of diepgewortelde stereotypen. Bonaci wijst erop dat de "elektrische signalen die ons lichaam produceert gevoelige informatie over ons bevatten. Informatie die we misschien niet bereid zijn te delen met de wereld." Haar zorg is dat "we die informatie kunnen blootgeven zonder dat we het ons realiseren."

Onlangs zijn ziekenhuizen in Engeland en Schotland slachtoffer geworden van een ransomware aanval. Hackers gebruikten de WannaCry-software die meestal via e-mail verspreid wordt als een documentbijlage. Nadat het document is geopend, tast de malware de hele computer aan en versleutelt het alle bestanden. In de ziekenhuizen had het als resultaat dat de personeelsleden hun computers en telefoons niet konden gebruiken en afspraken met hun patiënten moesten annuleren.

David Nickelson denkt dat het invoeren van een paar eenvoudige strategieën ziekenhuizen kan helpen om de veiligheid van hun patiënten te waarborgen. Volgens Nickelson moet cyberbeveiliging als een essentieel onderdeel worden beschouwd, vergelijkbaar met IT. Waar de IT zich focust op het delen van informatie, hebben ziekenhuizen cyberpersoneel nodig dat kritieke systemen kan beveiligen om informatie juist te beschermen. Door een zorgvuldige inschatting van de potentiële risico's kan zorgpersoneel ook kwetsbare gebieden aanwijzen zodat deze tijdig beschermd kunnen worden. Kate Kuhen, security vicepresident bij BT Americas Inc., vindt dat organisaties goed moeten begrijpen waar voor hen de dreiging zit. Ze adviseert om firewalls regelmatig te updaten en werknemers te waarschuwen geen verdachte e-mails te openen. Aangezien vrijwel elke organisatie digitaal gevaar loopt, moet ook ziekenhuispersoneel van die risico's op de hoogte worden gesteld.

Beveiligingsprogramma scores

Als je jouw beveiligingsprogramma zou evalueren, welk cijfer zou je het programma van jouw organisatie geven, waarbij "A" uitstekend en "F" tekortschietend is?



Bron: healthitsecurity.com/news/healthcare-ransomware-connected-devices-top-security-issues

2.0

AANVALLEN OP CRUCIALE INFRASTRUCTUUR

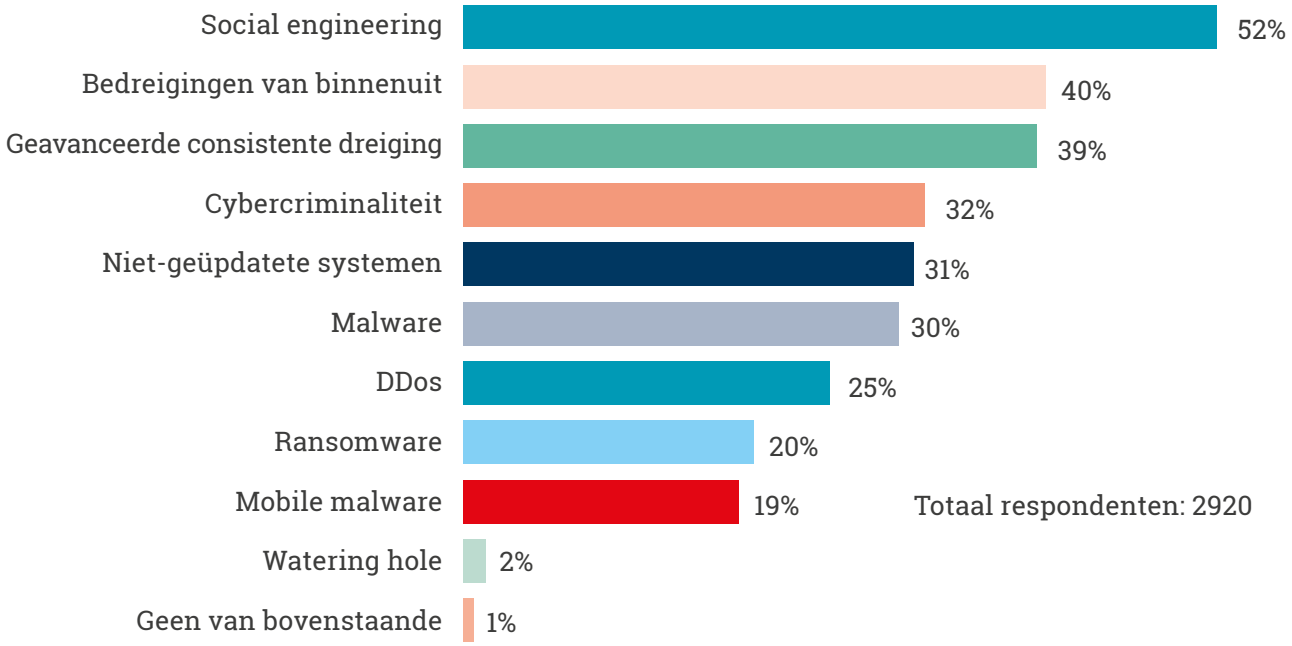
"De opkomst van cyberdreigingen op kritieke infrastructuur wijst erop dat industriële besturingssystemen op alle niveaus goed beveiligd moeten zijn tegen malware. Het is ook belangrijk op te merken dat, volgens onze observaties, de aanvallen vrijwel altijd beginnen met de zwakste schakel, namelijk mensen."

- Evgeny Goncharov, hoofd van het Critical Infrastructure Defense Department bij Kaspersky Lab

Slimme steden zijn slim, omdat ze gebruik maken van een breed scala aan sensoren en de connectiviteit van het IoT. Ze maken het leven makkelijker door zaken als intelligente verkeersleiding en slimme elektriciteitsnetten die zich automatisch aanpassen aan vraag en aanbod. Door technologie toe te passen in de infrastructuur van slimme steden, maken ze het leven van hun bewoners niet alleen eenvoudiger, maar ook comfortabeler. Deze toegenomen functionaliteit leidt echter ook tot een grotere kwetsbaarheid voor hacking.

Hackers vallen overheden, ziekenhuizen en politiediensten aan en hoewel cybersecurity bovenaan ieders prioriteitenlijst zou moeten staan, is hier nog maar weinig geld voor beschikbaar gesteld. Volgens een rapport van Deloitte en de National Association of State Chief Information Officers (NASCIO) investeren de meeste Amerikaanse staten extreem weinig - 2 procent van hun totale budget is een ruime schatting - in hun programma's voor cyberbeveiliging.

Grootste bedreigingen voor de organisatie



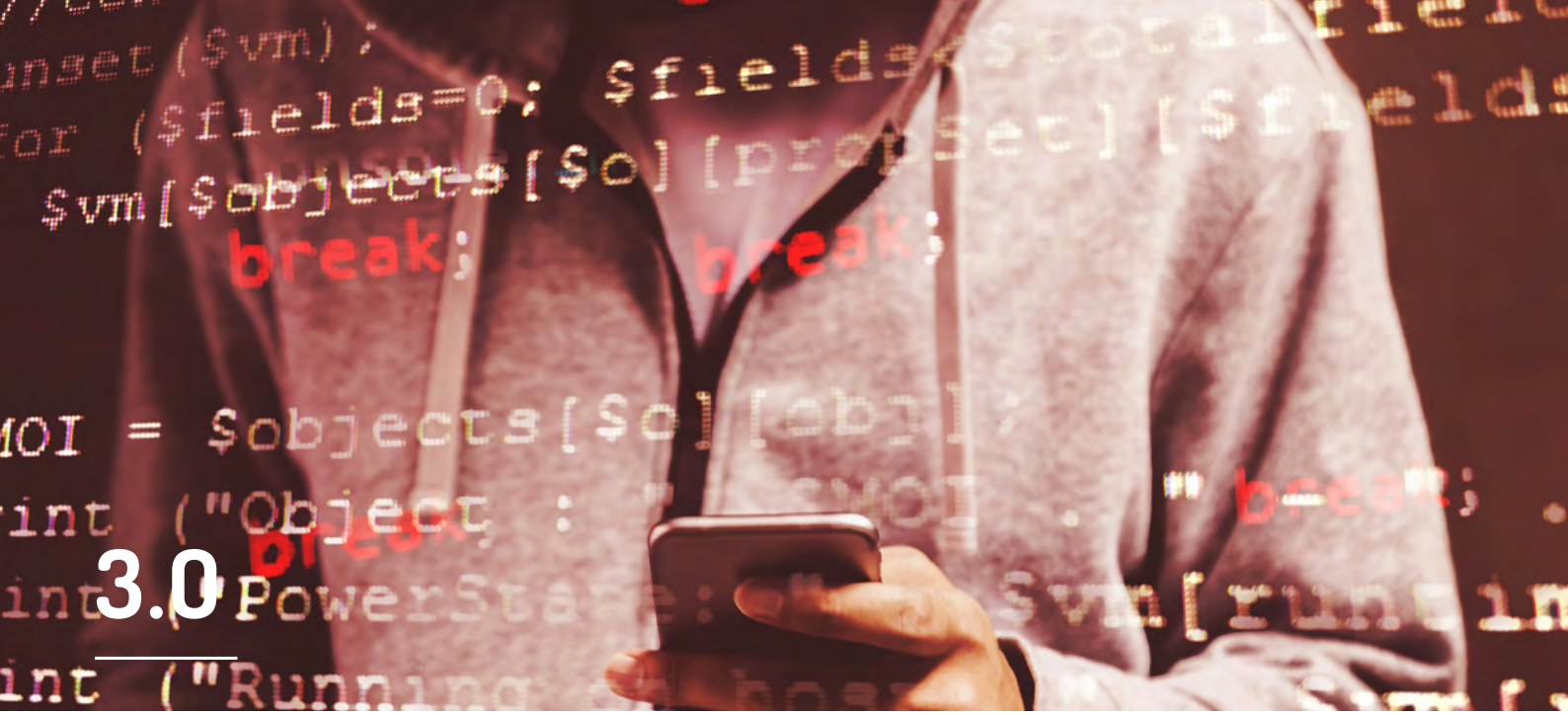
Bron: cioandleader.com

Omdat er over het algemeen relatief weinig tijd en aandacht wordt geïnvesteerd in het voorkomen van cyberaanvallen, komen ze in toenemende mate voor. Energienetten worden bijvoorbeeld steeds vaker het doelwit van hackers, wat tot grote stroomstoringen kan leiden. Een van die hacks vond in 2015 in Oekraïne plaats. Als gevolg daarvan zaten miljoenen burgers in de winter urenlang zonder elektriciteit. De hackers slaagden erin om de controle van alle computers die waren aangesloten op het energiecontrolesysteem van het bedrijf over te nemen met CrashOverride software, een populair hulpmiddel in de hackerswereld en de perfecte tool om netsystemen te saboteren. Ingenieurs van het regionale energiebedrijf keken hulpeloos toe hoe hackers stroomstoringen veroorzaakten door stroomonderbrekers uit te schakelen. Ondanks deze 'waarschuwing' was Oekraïne het jaar daarop wederom slachtoffer van een cyberaanval op energienetwerken. Op dezelfde manier kunnen hackers ook vervoerssystemen aanvallen, met dodelijke ongevallen als gevolg.

Door waterzuiveringsinstallaties te hacken kunnen cyberterroristen het watersysteem veranderen in een biologisch wapen dat miljoenen mensen kan besmetten. Vorig jaar is een groep hackers erin geslaagd om toegang te krijgen tot een waterbeheersysteem en de samenstelling van chemicaliën voor de behandeling van leidingwater te veranderen. Hoewel deze cyberaanval geen extreme gevolgen had, heeft het wel zwakke plekken in de infrastructuur van het waterbeheer aan het licht gebracht. Yoni Shohet, medeoprichter en CEO van SCADAfence, wijst erop dat "deze aanvallen bij bedrijven aanzienlijke financiële gevolgen hebben en leiden tot reputatieschade en verlies van concurrentievoordeel. Voor klanten kunnen deze inbreuken in het ergste geval dodelijk zijn. Stel je voor dat hackers met onze dagelijkse consumentenproducten knoeien, zoals medicijnen, voedsel en water. Dan zijn de potentiële gevolgen niet te overzien."

Voor de meeste hackers is geld verdienen – door middel van bijvoorbeeld cyberafpersing - het belangrijkste doel. Het slachtoffer moet dan losgeld betalen om de cyberaanval te stoppen. Hacks worden ook steeds heftiger en zijn steeds beter georganiseerd. Cybercriminelen verkopen hun diensten zelfs aan minder geavanceerde hackers op het Dark Web, en omdat je de benodigde middelen gemakkelijk online kunt krijgen, zijn de aanvallen eenvoudig uit te voeren.

Toch zijn niet alle hackers gemotiveerd door geld. In het Verenigd Koninkrijk is men bijvoorbeeld met name bezorgd dat terroristen elektronische systemen op luchthavens hacken om ze te kunnen omzeilen. Een dergelijke aanval heeft al plaatsgevonden in Turkije – daar werden de controlesystemen op de vertrekterminals van de luchthaven Istanbul Ataturk in 2013 gehackt, waardoor uiteraard een enorme chaos ontstond. Van dit soort situaties kunnen terroristen profiteren, met alle mogelijke gevolgen van dien.



3.0

HET IOT ONDER VUUR

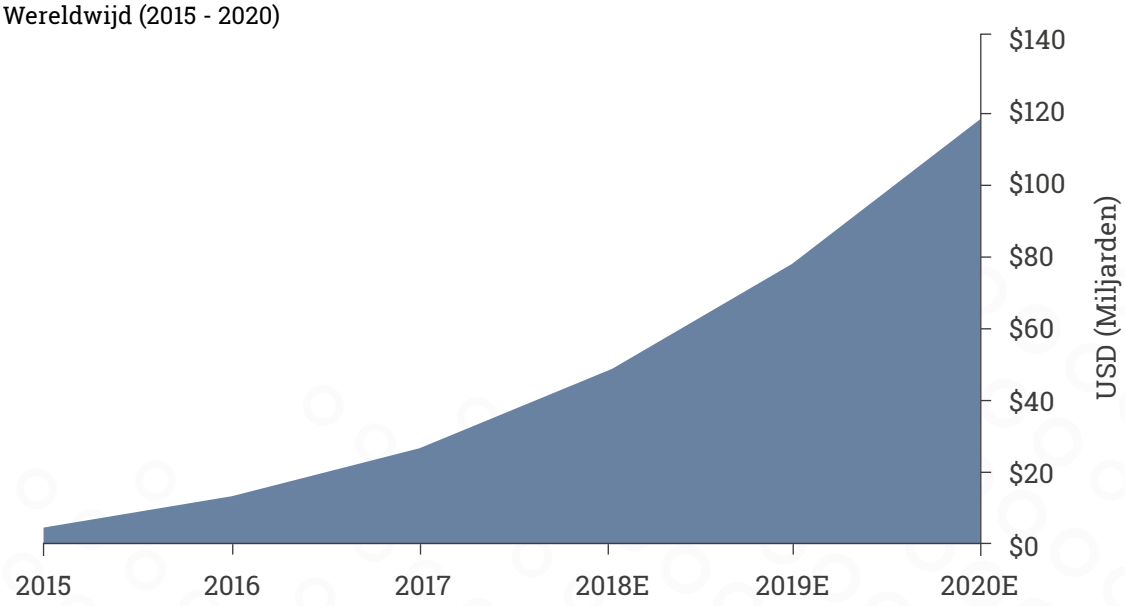
"Het staat buiten kijf dat de groei van het Internet of Things gestimuleerd wordt door de opwinding over de nieuwe functionaliteiten van internetverbinding. Beveiliging staat op de tweede plaats."

- Shuman Ghosemajumder, de chief technology officer bij Shape Security

Cisco, een wereldleider op het gebied van IT, voorspelt dat er tegen 2020 bijna 50 miljard apparaten aangesloten zullen zijn op het IoT, waardoor het de komende jaren een nog centraler deel van ons dagelijks leven zal vormen. Maar het gemak van al deze verbonden apparaten brengt ook veiligheidsrisico's met zich mee.

Geschatte markt cyberbeveiliging Internet of Things

Wereldwijd (2015 - 2020)



Bron: BI Intelligence estimates, 2015

Wetenschappers van de Universiteit van Binghamton en het Stevens Institute of Technology hebben aangetoond dat cybercriminelen wearables als smartwatches kunnen hacken en daaruit waardevolle gegevens kunnen halen. Het team van onderzoekers voerde een experiment uit met twintig mensen die smartwatches droegen. Het lukte hen om met behulp van een algoritme en de sensordata van de wearables persoonlijke wachtwoorden en PINcodes te hacken. De onderzoekers zijn van mening dat deze methode ook gebruikt kan worden als een slachtoffer zich bij een geldautomaat of een elektronisch slot bevindt.

Volgens een rapport van het National Computer Network Emergency Response Technical Team/Coordination Center of China (CNCERT/CC) worden slimme apparaten als webcams, drones en huishoudelijke apparaten steeds kwetsbaarder en zal het aantal cyberaanvallen de komende jaren toenemen. De directeur van het operations department van CNCERT, Yan Hanbing, wijst erop dat "er in smart devices – omdat ze klein zijn - niet veel beveiligingssoftware zit. Als er toch beveiligingsproblemen zijn, is het lastig om ze op te lossen met software-updates." Om de frequentie van cyberaanvallen te verminderen, voert China een wet op cyberbeveiliging in. Deze wet bepaalt de verantwoordelijkheden van de overheid en individuen in cyberspace en biedt richtlijnen voor het omgaan met potentiële digitale gevaren.

Naast smartwatches, telefoons en TV's kunnen zelfs apparaten als babyfoons gehackt worden. Het Nationaal Cybersecurity Centrum (NCSC) in het Verenigd Koninkrijk meldt: "De gegevens uit babyfoons zijn mogelijk niet intrinsiek waardevol en worden misschien niet op criminele fora verkocht, maar de data zou wel dusdanig waardevol voor het slachtoffer kunnen zijn dat hij of zij bereid is ervoor te betalen."

Stel je voor wat er kan gebeuren als ze speelgoed gaan hacken. De elf jaar oude Reuben Paul liet dit live zien tijdens de International One Conference in Nederland. Hij slaagde erin om met een goedkope Raspberry-Pi computer en genoeg kennis van de programmeertaal Python een robot teddybear te hacken en te besturen. Reuben toonde aan dat hij er verschillende boodschappen mee op kon nemen en de lichtjes van de beer aan- en uit kon zetten. Zijn vader gelooft dat kinderen tegenwoordig "spelen met tijdbommen, die iemand met kwade bedoeling en na verloop van tijd kan uitbuiten.

4.0

HET GEVAAR VAN 3D-, 4D- EN BIOPRINTERS

"Informatie- en communicatietechnologieën, kunstmatige intelligentie, 3D-printen en synthetische biologie zullen ons dagelijks leven ingrijpend veranderen en miljoenen mensen ten goede komen, maar het potentiële misbruik ervan kan ook ernstige schadelijke gevolgen hebben."

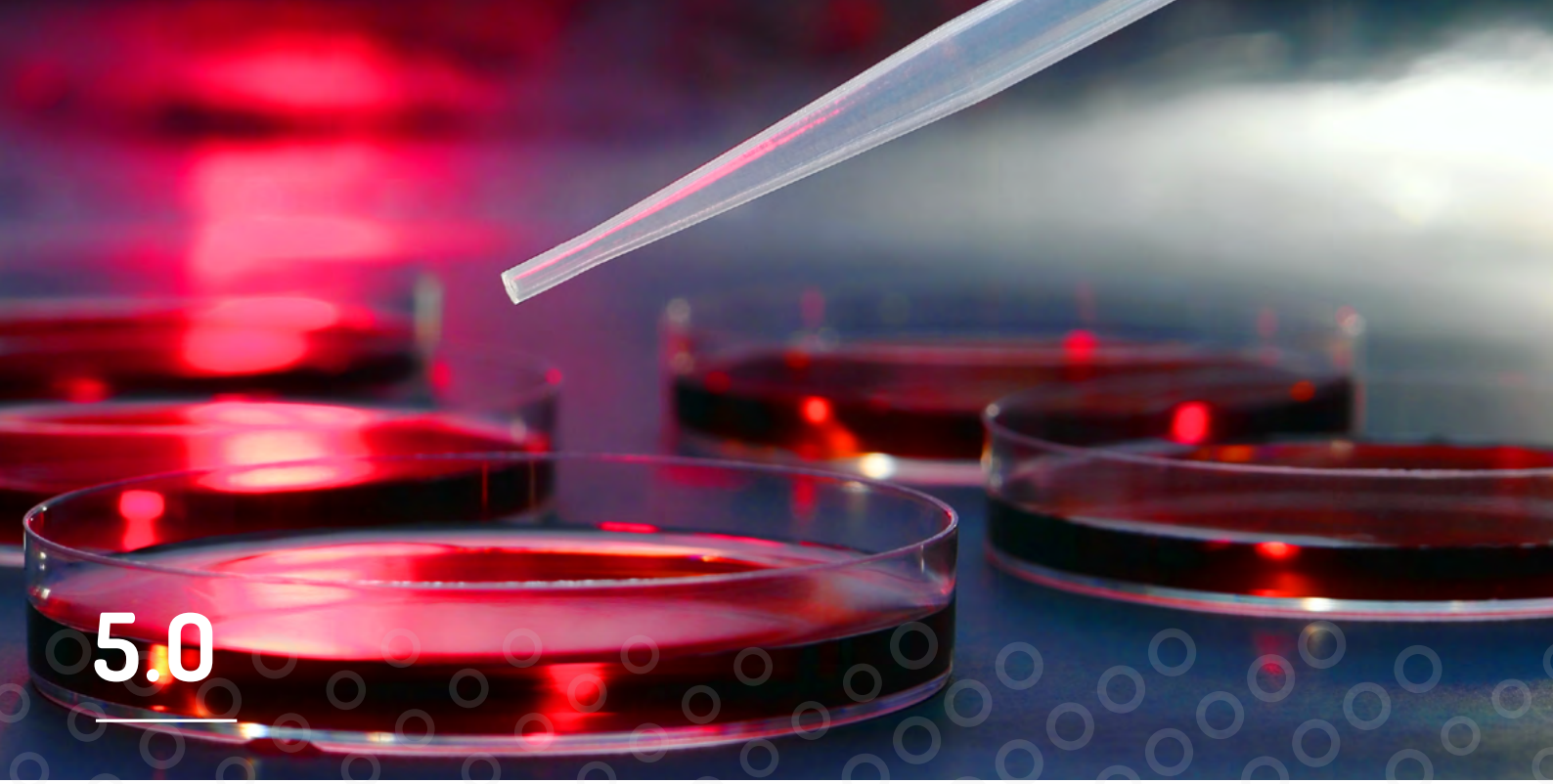
- Ban Ki-moon, UN Secretaris-Generaal

Met 3D-printtechnologie kunnen levens gered worden - denk bijvoorbeeld aan kunstmatige luchtwegen voor kinderen. Maar de technologie kan ook als wapen worden gebruikt bij het plegen van misdaad en terreurdaden. Met 3D-printtechnologie kunnen criminelen bijvoorbeeld ook fysieke beveiligingssystemen kraken of saboteren.

Veel beveiligingssystemen worden met vingerafdrukken ontgrendeld. Criminelen kunnen deze vingerafdrukken stelen door een replica van de hand in 3D te printen, waarmee ze kunnen inbreken in beveiligingssystemen zoals die bij luchthavens of banken. Anil Jain, hoogleraar aan Michigan State University, onthulde hoe eenvoudig dit is. Samen met zijn collega Nicholas Paulter van het National Institute of Standards and Technology (NIST) creëerde hij een 3D-geprinte hand die je als handschoen kunt dragen en gebruiken om vingerafdrukscanners te misleiden. Ze gebruikten een standaard 3D-printer en een rubberachtig materiaal om de textuur van de menselijke huid na te bootsen. Uit hun experiment bleek dat een 3D-printer in staat was om een handschoen te printen met nauwkeurige vingerafdrukken. Hiermee heeft Jain talloze gaten in de beveiliging van vingerafdrukscanners blootgelegd. Het is duidelijk dat verbeteringen in beveiligingsprotocollen van cruciaal belang zijn.

Bovendien brengt 3D-printtechnologie ook andere gevaren met zich mee. Het is bijvoorbeeld vrij eenvoudig om een online tutorial te vinden waarin uitgelegd wordt hoe je een vuurwapen kunt printen en in elkaar kunt zetten. Je zou denken dat dit een geavanceerd en complex proces is, maar dat is het niet en sommige regeringen nemen nu al voorzorgsmaatregelen om dit te voorkomen. Zo heeft de stad Philadelphia bijvoorbeeld regels ingevoerd die die het printen van wapens verbieden. Bovendien is er in Japan een man veroordeeld tot twee jaar gevangenisstraf voor het bouwen van een zogenaamd 'ZigZag' pistool met behulp van standaard CAD ontwerpsoftware.

De gevaren van 3D-geprinte vuurwapens trokken de aandacht van de secretaris-generaal van de VN Ban Ki-moon. In een toespraak voor de VN-Veiligheidsraad zei hij: "De enige manier om de menselijke, ecologische en existentiele vernietiging die deze wapens kunnen veroorzaken te voorkomen is door ze definitief uit te bannen."



5.0

BIOTECH TRANSFORMEERT TERRORISME

"Het is erg moeilijk om uitspraken te doen over de waarschijnlijkheid van bioterrorisme, maar de potentiële schade is enorm."

- Bill Gates, medeoprichter van Microsoft

De afgelopen jaren zijn we getuige geweest van de snelle ontwikkeling van biotechnologie. Als we kijken naar een aantal van die doorbraken, kunnen we er zeker van zijn dat de ontwikkelingen niet snel zullen stoppen. Maar doorbraken en uitvindingen in de geneeskunde, landbouw en voedselproductie kunnen helaas ook voor de verkeerde doeleinden gebruikt worden.

In de meest recente Worldwide Threat Assessment (Wereldwijde Bedreigingsbeoordeling) werd genbewerking opgenomen als nieuw potentieel massavernietigingswapen. In het verslag staat: "Gezien de wijdverbreide verspreiding, de lage kosten en snelle ontwikkelingstempo van deze technologie, kan het bewuste of onopzettelijke misbruik ervan verstrekkende gevolgen hebben voor de economische en nationale veiligheid."

Om dergelijk misbruik te voorkomen, ontwikkelt het Amerikaanse Defense Advanced Research Projects Agency (DARPA) een Safe Gene-programma dat veiligheidsmaatregelen promoot die in de biotechnologie moeten worden toegepast.

Dit geldt in het bijzonder voor CRISPR, een inmiddels alom bekende genbewerkingsmethode met een specifiek enzym die in 2012 bekend gemaakt werd. Het enzym – dat in bacteriën gevonden werd - kan worden gebruikt om genen in het DNA te modificeren. Online winkels als ODIN verkopen engineering kits voor $145 waarmee amateurwetenschappers thuis CRISPR genbewerking kunnen uitvoeren. In de verkeerde handen kunnen deze DIY-kits makkelijk als wapen gebruikt worden. Stel je voor dat terroristen iets ontwikkelen dat vergelijkbaar is met het H1N1-virus of Ebola!

Bill Gates maakt zich daar zorgen over. Tijdens het laatste World Economic Forum waarschuwt hij: "Het is erg moeilijk om uitspraken te doen over de waarschijnlijkheid van bioterrorisme, maar de potentiële schade is enorm."

6.0

HET REKRUTEREN VAN TERRORISTEN

"We moeten de boodschap verspreiden: Terroristen gebruiken social media om jonge kinderen te bereiken."

- John Carlin, assistent advocaat-generaal voor nationale veiligheid bij het Department of Justice in de VS

Het internet en social media bieden terroristen een scala aan platforms om berichten te verspreiden die razendsnel gedeeld kunnen worden. Zo gebruikt Islamitische Staat digitale platforms "om sociale netwerken op te bouwen en terreurdaden te crowdsourcen." Hun Twittervolgers maken even snel nieuwe accounts aan als de oude worden geblokkeerd. En ze hebben een uiterst efficiënte strategie ontwikkeld waarin bepaalde accounts originele content verspreiden en anderen het meest overtuigende materiaal delen. Op deze manier kunnen miljoenen zo niet miljarden mensen in zeer korte tijd bereikt worden.

Deskundigen maken zich hier zorgen over. Andrew Trabulsi van het Institute for the Future, een onderzoeksgroep zonder winstoogmerk, vergelijkt de rekruteringsinspanningen van terroristen met reclame en marketing. "Het is een conversietrechter, net zoals je ziet bij online reclame." Het idee is om dusdanig interesse te wekken voor hun ideologie dat mensen er daadwerkelijk bij betrokken raken.

"Als er een boodschap is die navolging krijgt, dan zal het de wereld in gaan," waarschuwt Nigel Inkster, een voormalig inlichtingenmedewerker, nu werkzaam bij het International Institute for Strategic Studies in Londen. "Wat het internet heeft veranderd is de snelheid waarmee een bericht wordt verzonden en hoe vaak het te zien is."

7.0

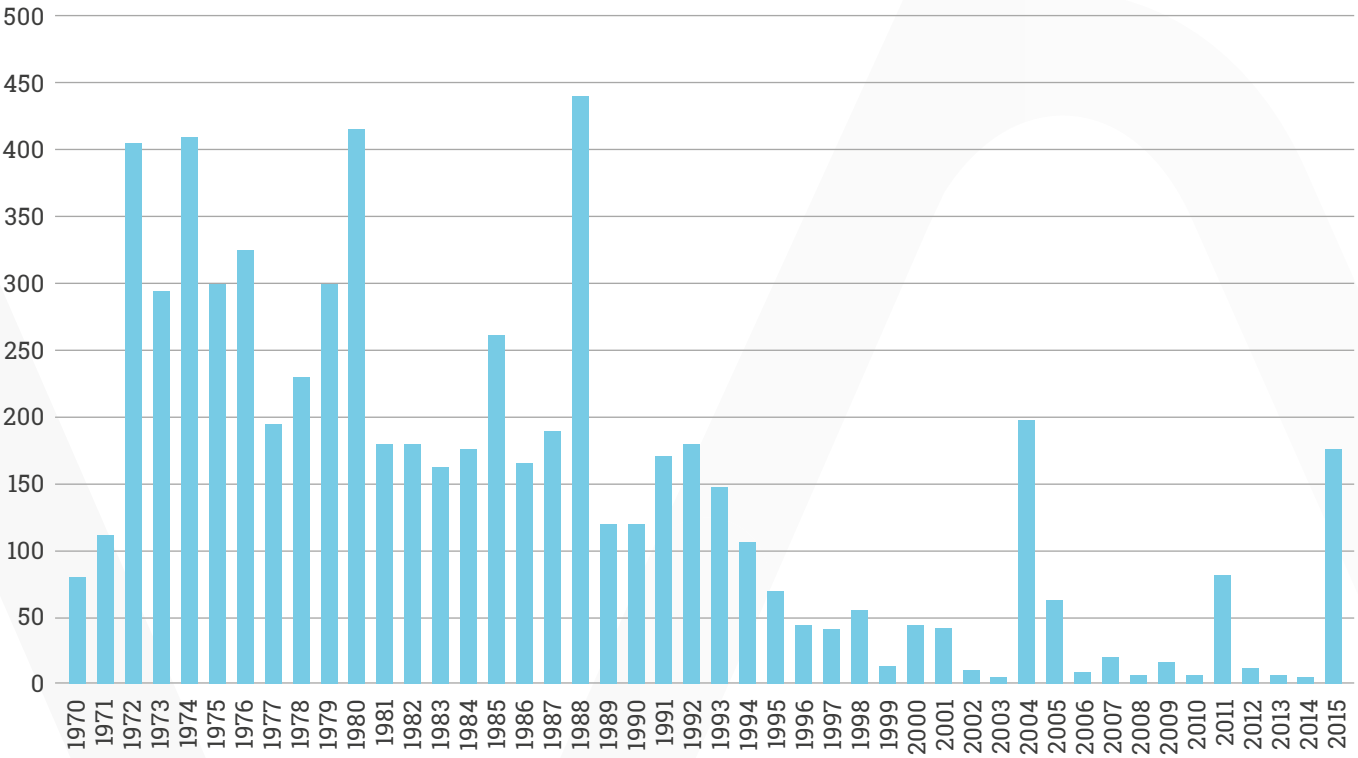
TERREUR ORGANISEREN

Terroristische organisaties gebruiken cyberspace ook voor rekrutering, communicatie en het plannen van aanvallen. Ze zijn verhuisd naar de digitale ruimte, mede omdat ze weten dat fysieke organisatie hen kwetsbaar maakt voor opsporing en arrestatie. Terreurcellen worden steeds kleiner, lokaler en hebben geen specifieke leider, waardoor het moeilijk wordt om de connectie tussen verschillende cellen te leggen of ze te uit te schakelen door belangrijke leiders te elimineren.

Zoals we de laatste tijd hebben kunnen zien, zijn de meest recente aanvallen lowtech: bestelwagens die in een menigte worden gereden of terroristen die met een mes willekeurige voorbijgangers aanvallen.

Er is geen formele training nodig voor deze gruwelijke daden en iedereen kan overal en op elk moment worden aangevallen."

Doden door terroristische aanvallen in West-Europa, 1970 – 2015



Bron: Datagraver.com

Deze aanpassingen in de tactiek weerspiegelen de realiteit van de zwakke plekken in terrorismebestrijding. Terroristen die alleen of in kleine cellen werken, zijn moeilijk te identificeren en te stoppen, omdat er geen patroon is waarmee mogelijke individuele terroristen opgespoord kunnen worden, vooral omdat het internet iedereen anonimiteit kan bieden. Dit is een enorm voordeel voor een terreurorganisatie of eenheid die zijn boodschap wil verspreiden en toch volledig onder de radar wil blijven.

"Het grootste voordeel van het internet is stealth," aldus John Arquilla, hoogleraar defensie-analyse aan de postuniversitaire marineopleiding. "Terroristen zwemmen in een oceaan van bits en bytes."

Ze maken gebruik van creatieve technieken die het internet tot een efficiënt en relatief veilig communicatiemiddel maken. Denk hierbij aan steganografie, een techniek om berichten te verbergen in grafische bestanden, en het zogeheten 'dead dropping', waarmee "informatie verzonden wordt via opgeslagen concept e-mails" in een account dat gedeeld wordt door verschillende terroristen.

Een andere handige manier waarop terroristen zich organiseren is via het Darknet. Deze 'duistere' gebieden van het internet worden niet geïndexeerd door standaard zoekmachines en bieden criminelen en terroristen daardoor de nodige onzichtbaarheid. Bijna alle sites op het Darknet verbergen de identiteit en locatie van hun gebruikers met behulp van de encryptietool Tor. De locatie wordt in feite 'gespoofd', waardoor het lijkt alsof de gebruiker in een ander land is. De locatie is daardoor zelfs voor de meest geavanceerde inlichtingendiensten vaak niet te achterhalen.

Laith Alkhouri, medeoprichter van Flashpoint, een bedrijf dat Darknet data monitort en contextualiseert, zegt: "Door het Darknet in de gaten te houden kun je sentiment in de jihadistische gemeenschap meten, waar fundamentalisten ideeën voor het eerst uitdragen en uitbroeden."

8.0

HACKTIVISME

Hacktivisme is het voor politieke of andere doeleinden ondermijnend gebruik van computers en computernetwerken. De FBI definieert terrorisme als een activiteit met een de volgende drie kenmerken: "Het moet lijken te zijn bedoeld om (i) een burgerbevolking te intimideren of te dwingen iets te doen; (ii) het beleid van een regering te beïnvloeden door intimidatie of dwang; of (iii) het gedrag van een regering te beïnvloeden door middel van massavernietiging, moord of ontvoering."

Uit deze definitie kunnen we opmaken dat hacktivisme, hacken met politieke motieven, waarschijnlijk geen terrorisme is, hoewel de grens wazig is. In tegenstelling tot cybercriminelen die computernetwerken hacken en data stelen om geld te verdienen, doen de meeste hacktivisten het niet voor financieel gewin. Zij zien het als een manier om onrechtvaardigheid te bestrijden. "Het is digitale ongehoorzaamheid. Het is hacken met een hoger doel," zegt Dan Lohrmann, de chief security officer voor Security Mentor, een nationaal veiligheidstrainingsbureau dat samenwerkt met staatsoverheden in de VS.

En iedereen is een potentieel doelwit, van regeringen tot drugsdealers en van politiediensten tot ziekenhuizen. Doug Robinson, de uitvoerend directeur van de National Association of State Chief Information Officers (NASCIO), zegt: "Sommigen zien hacktivisme als iets onschuldigs en denken dat het gewoon een vorm van protest is. Maar het kan zeer ontwrichtend zijn. Het is een overtreding."

Maar hoe bestrijd je hacktivisme?
Om de kans de kans te verkleinen dat organisaties het slachtoffer worden van hacktivisme, moeten ze volgens Deloitte over een sterk bewakings- en opsporingsvermogen beschikken, gekoppeld aan een adequaat responsteam. Technische middelen en deskundig personeel zijn de belangrijkste componenten van een effectieve firewall. Ze benadrukken dat een strikte bewaking en detectie niet efficiënt zijn tenzij de respons solide is. Als een bewakingssysteem bijvoorbeeld een alarm activeert en er is niemand die de situatie kan onderzoeken, dan schiet de firewall tekort.

9.0

KI, DRONES EN ROBOTS: GOED TEGEN KWAAD

"Een gevechtsrobot kan uiteindelijk de menselijke prestaties overtreffen als het gaat om de naleving van het internationaal humanitair recht. Dat komt dan neer op het redden van burgerlevens en is dus een humanitaire operatie. Als dit inderdaad haalbaar is kan er zelfs een morele verplichting bestaan voor het gebruik ervan."

- Ronald C. Arkin, directeur van het Mobile Robot Laboratory en Associated Dean voor onderzoek bij het College of Computing aan het Georgia Institute of Technology

Men verwacht dat kunstmatige intelligentie (KI) de verdedigingstechnologie zal hervormen, maar er zijn ook diverse uitdagingen. Het meest voor de hand liggende voordeel van het gebruik van dit soort technologie is de vermindering van het aantal militaire slachtoffers. DOGO, bijvoorbeeld, ontworpen door General Robotics Ltd. en door *Defense News* omschreven als 's werelds eerste intrinsiek gewapende tactische gevechtsrobot, zou een revolutie teweeg kunnen brengen in de manier waarop militaire eenheden wereldwijd terreurbestrijding uitvoeren. DOGO, die als verkennings- of moordrobot functioneert, kan - indien nodig - ongeveer vier uur op een batterijlading werken werken.

Klik voor video

Aangezien KI-systemen niet immuun zijn voor malware en virussen, kan dit soort geavanceerde oorlogsvoering ook een bedreiging vormen voor burgers. Ook zouden terroristen de zwakke punten van KI kunnen misbruiken om het te herprogrammeren door firewalls en andere veiligheidssystemen te omzeilen. De potentiële gevolgen van cyberaanvallen met behulp van KI-technologie zijn niet te overzien. Stel je voor wat er zou kunnen gebeuren als een geavanceerde terreurcel het voor elkaar krijgt om de controlesystemen van nucleaire, biologische of chemische wapens te hacken.

Deskundigen maken zich zorgen over het feit dat we KI implementeren voordat we de mogelijke problemen en valkuilen goed hebben beoordeeld. Mary Cummings, geassocieerd hoogleraar aan Duke University en directeur van Duke's Humans and Autonomy Laboratory, schrijft: "Gezien de huidige mate van commerciële ontwikkeling van drones en andere robotsystemen zijn er andere belangrijke overwegingen. Denk aan de mogelijk verborgen gevolgen van bedrijven en landen die KI-technologieën haastig op de markt brengen."

De snel evoluerende systemen zorgen er echter voor dat "autonome systemen voor militairen en burgers geaccepteerd worden en normaal gevonden worden" voordat we weten hoe we om moeten gaan met de gevolgen ervan. *The Sun* meldde dat meer dan 1.500 vooraanstaande wetenschappers een brief hebben ondertekend waarin "werd opgeroepen om moordrobots te verbieden en een einde te maken aan de wapenwedloop op het gebied van kunstmatige intelligentie." En professor Stephen Hawking zegt dat "overheden bezig lijken te zijn met een KI-wapenwedloop, waarbij vliegtuigen en wapens met intelligente technologieën worden ontworpen. Projecten die de mensheid rechtstreeks ten goede komen, zoals betere medische screening, lijken een lagere prioriteit te hebben."

10.0

CRIME-AS-A-SERVICE

"Vandaag de dag kan bijna iedereen cybercrimineel worden. Dit zet wetshandhavingsinstanties steeds meer onder druk. We moeten onze nieuwe kennis over het online functioneren van georganiseerde misdaad gebruiken om meer internationale operaties te starten. We moeten ervoor zorgen dat onderzoeken naar betaalkaartfraude en online kindermisbruik niet ophouden bij nationale grenzen."

- Cecilia Malmström, de EU-commissaris voor binnenlandse zaken

De meeste bedrijven zijn zich bewust van het gevaar van cyberaanvallen, maar er is weinig bekend over Crime-as-a-Service (CaaS) of cybermisdaad-als-dienst. In het verleden had iemand met criminele bedoelingen speciale vaardigheden of kennis nodig om een aanval uit te voeren. Nu is er een verrassend breed scala aan hulpmiddelen en technologieën online beschikbaar - van kits om mensen uit te buiten tot ransomware waarmee cybercriminelen zonder technische expertise zelf toch een aanval kunnen uitvoeren. Kits die de ontwikkeling en levering van malware automatiseren zijn een levendige handel geworden met hun eigen vraag- en aanbodketen.

Ransomware is bijvoorbeeld het snelst groeiende segment van CaaS vanwege de waarde van de data. Slachtoffers zijn vaak bereid om te betalen om iets dat privé, compromitterend of belangrijk is, terug te krijgen. In een recent rapport van McAfee staat: "Ransomware is financieel lucratief met weinig kans op arrestatie."

Sommige aanvallers maken gebruik van deze ransomware-als-dienst omdat ze daarmee minder risico lopen. "Je kunt de infrastructuur van iemand anders gebruiken, waardoor je niet alleen een extra laag legt tussen jou en je slachtoffers, maar ook tussen jou en de wetshandhavers die proberen je op te sporen," legt Rick Holland, vicepresident van strategie voor Digital Shadows, uit.

11.0

WAT KUNNEN WE DOEN OM ONSZELF TE BEVEILIGEN?

Naarmate de connectiviteit toeneemt, brengt onze afhankelijkheid van technologie nieuwe risico's met zich mee. Helaas zijn terroristen en criminelen op zoek naar nieuwe manieren om deze kwetsbaarheden uit te buiten, wat door cyberspace relatief eenvoudig gemaakt wordt. De anonimiteit en het wereldwijde bereik stellen individuen met slechte bedoelingen in staat om in een tweede wereld - waar wetten gewoonweg niet van toepassing lijken te zijn – ongestoord hun gang te gaan. Overheden zoeken continu naar manieren om hackers, criminelen en terroristen op te sporen, maar pogingen om deze criminelen te ontmaskeren leiden ook tot uitdagingen rond privacy.

Het uitzetten van een breed net om deze criminelen te vangen dreigt ook onze elementaire rechten te ondermijnen en overheden zijn zich daarvan bewust. De speciale rapporteur voor het recht op privacy (SRP) van de Verenigde Naties, Joseph Cannataci, heeft op 8 maart 2017 de Mensenrechtenraad een verslag voorgelegd over de "eerste stappen in de richting van meer privacyvriendelijk overheidstoezicht."

Het verslag benadrukt het belang van op feiten gebaseerde 'proportionaliteit'. Dat wil zeggen dat er een maatstaf moet zijn waarmee het risico van inbreuk op de privacy van een maatregel wordt beoordeeld in verhouding tot de mate waarop de maatregel het risico op terrorisme vermindert:

"De complexiteit van gegevensstromen over traditionele soevereine grenzen leidt tot volledig nieuwe uitdagingen.

Er bestaat een verdrag omtrent cybercriminaliteit, dat door 25 procent van de VN-lidstaten is ondertekend, maar het heeft alleen betrekking op de strafrechtelijke sector. Het heeft geen betrekking op de nationale veiligheid of op toezicht dat wordt uitgeoefend in naam van de nationale veiligheid. Een internationale autoriteit zou een equivalent kunnen toekennen van een internationaal surveillancebevel of een internationaal gegevensbevelschrift dat te handhaven is in cyberspace."

Dr. Daniel Prince, geassocieerd directeur en manager voor zakelijke partnerschappen voor Security Lancaster, het centrum voor veiligheidsonderzoek van de Universiteit van Lancaster, benadrukt dat het delen van informatie essentieel is. "De National Cyber Forensics Training Alliance (NCFTA) in de VS, het sectoroverschrijdende centrum voor veiligheids- en beveiligingscommunicatie (CSSC) en het National Cyber Security Centre (NCSC) in het VK zijn drie van de beste voorbeelden van hoe informatie het best uitgewisseld kan worden. De NCFTA is een non-profitorganisatie die een informatiedelingscentrum beheert met geïntegreerde wetshandhavingsinstanties, universiteiten en bedrijven."

Het is duidelijk dat we een juridisch instrument nodig hebben om cyberterrorisme en cybercriminaliteit te bestrijden. Vermindering van de risico's van hightech aanvallen "zou goed zijn voor burgers, overheden, privacy en het bedrijfsleven."

CONCLUSIE

Internetverbinding is de nieuwe norm geworden in het dagelijks leven en steeds meer apparaten krijgen internetconnectiviteit. Bovendien hebben medische implantaten en kritieke infrastructuur het IoT nodig om goed te functioneren. Maar onze huidige veiligheidssystemen zijn kwetsbaar voor de gevaren die in het digitale universum op de loer liggen. Cyberterroristen en cybercriminelen proberen de kwetsbaarheden van deze hyperconnectiviteit genadeloos uit te buiten. Alleen door de gezamenlijke inzet van deskundigen en overheden kunnen we er hopelijk voor zorgen dat we geen slachtoffer worden van cybermisdaad of -terrorisme.

BIBLOGRAFIE

Acharya, Amrit P., and Arabinda Acharya, "Cyber-terrorism and biotechnology," Foreign Affairs, 1 June 2017, accessed 28 June 2017.

Acharya, Amrit P., and Arabinda Acharya, "Dangerous combination: Is CRISPR a potential weapon for terrorists?" Genetic Literacy Project, 8 June 2017, accessed 28 June 2017.

Alec, "Ban Ki-moon: 'digital technologies like 3D printing have the potential for massive destruction'," www.3ders.org, 25 Aug 2016, accessed 28 June 2017.

Arkin, Ronald C., "Warfighting robots could reduce civilian casualties, so calling for a ban now is premature," IEEE SPECTRUM, 5 Aug 2015, accessed 3July 2017.

Asher, Jeff, and Rob Arthur, "Inside the algorithm that tries to predict gun violence in chicago," The New York Times, 13 June 2017, accessed 28 June 2017.

Basulto, Dominic, "From hacking computers to hacking humans," Big Think, n.d., accessed 28 June 2017.

Bergal, Jenni, 'WannaCry' ransomware attack raises alarm bells for cities, states," Route Fifty, 19 May 2017, accessed 28 June 2017.

Bergal, Jenni, "Hacktivists launch more cyber-attacks against local, state governments," PBS NEWSHOUR, 10 Jan 2017, accessed 28 June 2017.

Bhunia, Priyankar, "China CERT report highlights rise in cyberthreats associated with IoT devices and networked industrial systems," Open Gov, 23 Apr 2017, accessed 28 June 2017.

Bhunia, Priyankar, "UN expert calls for international law and multilateral treaties for balancing privacy rights and security requirements," OpenGov, 9 Mar 2017, accessed 28 June 2017.

Blain, Loz, "Do-it-yourself CRISPR genome editing kits bring genetic engineering to your kitchen bench," New Atlas, 11 Nov 2015, accessed 28 June 2017.

Brown, Jennings, "DARPA wants to block national security threats posed by gene editing," Vocativ, 13 Sep 2016, accessed 28 June 2017.
Brown, Kristen V., "Bill Gates warns that damage caused by bioterrorism could be 'very, very huge'," Gizmodo, 23 Jan 2017, accessed 28 June 2017.

https://www.cfr.org/backgrounder/terrorists-and-internet, accessed 3 July 2017.

Choudhury, Rummi, "Connected devices on IoT led to major cyberattack," MISCO.co.uk, 24 Oct 2016, accessed 3 July 2017.

Cummings, Mary L., "Artificial Intelligence and the Future of Warfare," pdf., 26 Jan 2017, accessed 28 June 2017.

Curtis, Sophie, "Eleven-year-old 'cyber ninja' hacks a teddy bear to show how toys can be weaponised to spy on kids," Mirror, 17 May 2017, accessed 28 June 2017.

https://www2.deloitte.com/content/dam/Deloitte/us/Documents/risk/us-aers-hacktivism.pdf, accessed 28 June 2017.

Dhaliwal, Sukhmani, "The future of cyber terrorism: Where the physical and virtual worlds converge," International Journal of Scientific Research and management (IJSRM), 9 Sep 2016, accessed 28 June 2017.

http://www.economist.com/news/international/21723106-some-criticism-unfair-there-more-they-could-do-tech-giants-are-under-fire, accessed 27 June 2017.

Egan, Matt, "What is the Dark Web and Deep Web?" Tech Advisor, 19 June 2014, accessed 3 July 2017.

Fenske, Sean, "Pacemaker Hacked...or Was It?" Medical Design Technology, 9 Aug 2015, accessed 5 July 2017.

Fletcher, Ian, "Smartwatches reveal bank card PIN numbers with 'alarming accuracy' in disturbing cyber crime experiment," Mirror, 7 July 2016, accessed 28 June 2017.

Goldstein, Phil, "Businesses that rely on smart city infrastructure could be vulnerable after cyberattacks," BizTech Magazine, 21 June 2017, accessed 27 June 2017.

Goodin, Dan, "In not-too-distant future, brain hackers could steal your deepest secrets," Ars Technica, 2 Jan 2017, accessed 27 June 2017.

Gornall, Jonathan, "The heart pacemakers at risk from hackers: Sound far-fetched? Security experts are treating it deadly seriously," Daily Mail, 29 Sep 2015, accessed 5 July 2017.

Graham, Chris, "NHS cyber attack: Everything you need to know about 'biggest ransomware' offensive in history," The Telegraph, 20 May 2017, accessed 5 July 2017.

Greenberg, Andy, "How an entire nation became Russia's test lab for cyberwar," Wired, 20 June 2017, accessed 27 June 2017.

Greenberg, Andy, "Watch hackers take over the mouse of a power-grid computer," Wired, 20 June 2017, accessed 27 June 2017.

Gregg, Michael, "'Cyber sabotage' could be the next big crime wave,'" Huffington Post, 20 June 2017, accessed 27 June 2017.

Hamill, Jasper, "Killing machine terrorists 'actively seeking' to build deadly army of intelligent killer robots, UN warns," The Sun, June 29 2016, accessed 28 June 2017.

Heires, Katherine, "Terror Tech," RISK MANAGEMENT, 1 Dec 2016, accessed 3 July 2017.

Herberger, Carl, "Cybersecurity in the real world: 4 examples of the rise of public transportation systems threats," Radware Blog, 21 Apr 2016, accessed 3 July 2017.

https://www.helpnetsecurity.com/2014/09/30/the-crime-as-a-service-business-model/, accessed 3 July 2017.

Hill, Michael, "Water treatment plant hit by cyber-attack," Info Security, 24 Mar 2016, accessed 5 July 2017.

Holt, Thomas, "Here's how terrorist groups use technology to recruit new members," Business Insider, 28 Apr 2016, accessed 27 June 2017.

Hope, Jason, "The rise of IoT and security issues," business.com, 24 Feb 2017, accessed 28 June 2017.

http://resources.infosecinstitute.com/the-role-of-technology-in-modern-terrorism/, accessed 3 July 2017.

http://ippreview.com/index.php/Blog/single/id/481.html, accessed June 27 2017.

Isaac, Lauren, "Isis recruitment in the cyber world," Social Justice Solutions, 4 May 2016, accessed 27 June 2017.

James E. Hatte, "Does hacktivism really equal terrorism?" Hack Read, 2016, accessed 27 June 2017.

Leyden, John, "Water treatment plant hacked, chemical mix changed for tap supplies," The Register, 24 Mar 2016, accessed 5 July 2017.

Lohrmann, Dan, "The dramatic rise in hacktivism," TechCrunch, 22 Feb 2017, accessed 28 June 2017.

Newman, Lily Hay, "Medical devices are the next security nightmare," Wired, 3 Feb 2017, accessed 27 June 2017.

Perry, Philip, "Low-cost gene editing could breed a new form of bioterrorism," Big Think, 2 Oct 2016, accessed 28 June 2017.

Pettifor, Tom, "Hackers could target TVs, mobiles and fitness trackers say security chiefs," Mirror, 14 Mar 2017, accessed 28 June 2017.

http://www.pdmodels.co.uk/en/blog/3dprinting/3d_printing,_terrorism_and_organised_crime,accessed 28 June 2017.

http://www.pdmodels.co.uk/en/blog/3dprinting/gun_manufacture_problem, accessed 28 June 2017.

BIBLOGRAFIE

Qichao, Zhu, "AI and the next revolution in military defence: China Daily columnist," THE STRAITS TIMES, 6 June 2017, accessed 28 June 2017.

http://www.un.org/en/sc/ctc/news/2014-03-24_Terrorists_act_alone.html, accessed 3 July 2017.

http://www.rappler.com/newsbreak/iq/173085-fast-facts-cyber-sedition, accessed 27 June 2017.

Riley-Smith, Ben, Patrick Sawer, Nicola Harley, and Nick Allen, "Airports and nuclear power stations on terror alert as government officials warn of 'credible' cyber threat," The Telegraph, 2 Apr 2017, accessed 27 June 2017.

Robinson, Rick M., "Cybercrime-as-a-Service poses a growing challenge," SecurityIntelligence, 4 Sep 2016, accessed 28 June 2017.

Romero, Alexis, "Government to arrest people for cyber sedition, says DICT," philStar Global, 13 June 2017.

Rooth, Ben, "Collaboration is key to stop cyber crime," Manchester Evening News, 12 June 2017, accessed 28 June 2017.

Schwartz, Matthew J., "Cybercrime-as-a-Service economy: stronger than ever," Bank Info Security, 14 Sep 2016, accessed 28 June 2017.

Scott, Clare, "Could 3D printed fingerprints help criminals break through security? MSU researchers demonstrate it's possible," 3dprint.com, 21 Oct 2016, accessed 28 June 2017.

Seals, Tara, "40% of ICS, critical infrastructure targeted by cyberattacks," info security magazine, 29 Mar 2017, accessed 3 July 2017.

Siwicki, Bill, "Is your hospital hacker bait? Here's how to change that," Healthcare IT News, 14 June 2017, accessed 27 June 2017.

Snell, Elizabeth, "Overcoming the healthcare cybersecurity workforce shortage," Health IT Security, 20 June 2017, accessed 3 July 2017.

Sweet, Carson, "The rise and risk of IoT in healthcare," The Stack, 8 May 2017, accessed 27 June 2017.

Tal, David, "Forecast | Future of organized crime: Future of crime P5," Quantumrun, 3 Nov 2016, accessed 28 June 2017.

Taylor, Harriet, "Most young terrorist recruitment is linked to social media, said DOJ official," CNBC, 5 Oct 2016, accessed 27 June 2017.

UN News Centre, "At Security Council, Ban calls for eradicating weapons of mass destruction 'once and for all'," www.un.org, 23 Aug 2016, accessed 3 July 2017.

Wagner, Daniel, "Why new laws won't stop cyber terrorism," Huffpost, 7 June 2017, accessed 28 June 2017.

Wilson, Lauren, "Crime as a service: the gritty details & how to prevent it," ThreatSTOP, 12 Jan 2017, accessed 28 June 2017.

Wordsworth, Rich, "Could 3D-printed organs be medicine's next grisly black market?" Wired, 26 Sep 2016, accessed 28 June 2017.

Bezoek richardvanhooijdonk.com voor interessante content, video's en boekingen.

Deze whitepaper is ook in het Engels verkrijgbaar.
Bezoek onze website.

Dutch office

Hoofdstraat 252
3972 LK Driebergen
Netherlands
t + 31 85 3030792
m + 31 6 41330000
richard@vanhooijdonk.com

UK office

Kemp House, 152 City Road
London EC1V 2NX
United Kingdom
t + 31 85 3030792

RICHARD VAN HOOIJDONK
TRENDWATCHER & FUTURIST