‘Cybercriminaliteit is exponentieel, geautomatiseerd en driedimensionaal’.

Er is alle reden om enthousiast te zijn over de digitale revolutie, maar net als alle nieuwe technologieën heeft die ook keerzijden. Cybercriminaliteit is er een van. Marc Goodman heeft een duidelijke visie op hoe criminaliteit zich in de toekomst kan ontwikkelen. Na een carrière bij de politie werkte Goodman tien jaar voor Interpol. Momenteel is hij ‘futurist in residence’ bij de FBI. Volgens Goodman is cybercriminaliteit exponentieel, geautomatiseerd en driedimensionaal.

Exponentieel
Moore's Law, die stelt dat computerchips ongeveer elke twee jaar dubbel zo snel worden, heeft niet alleen invloed op legale activiteiten. Het effect is ook te merken bij criminaliteit, zegt Goodman. "Criminaliteit was altijd een goede start-up. Je kocht een mes of een pistool, je verstopte je in een donkere straat en je zei: 'Geef me je geld'. Het probleem met dat businessmodel was de schaal. Je kunt nu eenmaal maar een beperkt aantal mensen per dag beroven. De locomotief was al technologie die boeven hielp om meer mensen te beroven. Internet maakt het mogelijk om honderden miljoenen accounts te compromitteren, zoals in de praktijk al is gebeurd. En ook de eerste bankroof van een miljard hebben we al gehad: bij de Carbanack-aanval stalen criminelen geld van meer dan 100 banken in 30 landen. In 2019 zal de wereldwijde impact van cybercriminaliteit twee biljoen dollar zijn."

Criminelen doen natuurlijk wat ze willen, zegt Goodman. "Ze hoeven geen toestemming te vragen of formulieren in te vullen. En ze handelen per definitie immoreel. Rob Ford, de voormalige burgemeester van Toronto, werd door drugdealers gefilmd terwijl hij crack gebruikte. Die video werd op Indiegogo geplaatst en zou worden vertoond als er via crowdfunding meer dan 200.000 dollar werd verzameld. Dat is dus gelukt. Russische hackers zijn erin geslaagd om prepaid bankkaarten te kopiëren, de limiet ervan te verwijderen en de wereld rond te sturen. Binnen tien uur werd er in 27 landen 45 miljoen dollar opgenomen."

"Er zitten nu slechteriken in het systeem waarvan we nog niets weten."

Geautomatiseerd
Misdaad is niet alleen veelomvattender geworden, maar ook makkelijker. "Je hoeft geen meesterhacker te zijn om in een computersysteem te komen", zegt Goodman. "Er is software die dat voor je doet, en je kunt hackingservices kopen. Criminaliteit is geautomatiseerd geworden. De mens verdwijnt naar de achtergrond en de software regelt het zelf. Er wordt al kunstmatige intelligentie ingezet bij cyberaanvallen. Als je eenmaal een supersterke computer hebt, is het een kwestie van programmeren. Stel dat we uiteindelijk een computer hebben die de gelijke is van het menselijk brein, maar dan veel sneller, en dat zo'n systeem kunstmatig intelligent wordt. Stephen Hawking heeft gezegd dat de ontwikkeling van volledige *artificial intelligence* het einde van de mensheid zou kunnen betekenen."

Maar ook zonder een supercomputer kunnen criminelen kunstmatige intelligentie gebruiken. "Pedro Bravo, een achttienjarige student aan de universiteit van Florida, vermoordde zijn huisgenoot. Toen de politie de verdwijning van de huisgenoot onderzocht, namen ze Pedro's iPhone in beslag. Ze kwamen zo ook de opdrachten tegen die Pedro had gegeven aan Siri, de personal assistent van de iPhone die antwoord geeft op gesproken vragen. Uit analyse bleek dat Pedro letterlijk aan Siri had gevraagd waar hij het beste een lijk kon begraven."

"In 2019 zal de wereldwijde impact van cybercriminaliteit twee biljoen dollar zijn."

Kwetsbaar in drie dimensies
Tot nu toe was de dreiging van cybercriminaliteit altijd tweedimensionaal: op het computerscherm. Maar, waarschuwt Goodman, computers komen de fysieke wereld in en dat heeft consequenties. "We kunnen de zaken die we nu online hebben staan al niet eens beschermen. Technisch kan internet straks 78 quadriljard mogelijke verbindingen aan. Zo'n getal maakt duidelijk dat we pas aan het prille begin staan van de internetrevolutie. We hebben geen idee waar het naar toe gaat. In een moderne auto zitten meer dan 250 computerchips. Van de gestolen auto's in Londen was in 2014 60% gehackt. Een auto is een computer waar je in rijdt, net als een vliegtuig een computer is waar je in vliegt. Hoe meer verbindingen we hebben, hoe kwetsbaarder we worden."

Onder vuur
De bestrijding van cybercriminaliteit is niet alleen een kwestie van technologie, zegt Goodman. "Technologie is net als vuur: je kunt het gebruiken om je warm te houden, om je eten op te koken, of om het dorp naast dat van jou af te branden. Met technologie die zich volgens de wet van Moore ontwikkelt, groeit de kans om exponentieel goed te doen, of exponentieel slecht. Als je wilt voorkomen dat mensen misbruik van je maken, dan zul je de technologie moeten begrijpen."

Daarnaast zijn er eenvoudige maatregelen die vaak niet worden genomen. Goodman zelf noemt er een aantal in zijn boek *Future crimes*. "Daarmee reduceer je je persoonlijke cyberrisico met 85%. Helaas wordt bij zakelijke cyberdreiging slechts 5% van alle virussen

Marc Goodman
Marc Goodman is een van de belangrijkste beveiligingsexperts in de wereld als het gaat om cybercriminaliteit, cyberterrorisme en informatieoorlogen. Zijn ervaring berust op zijn werk met organizaties als Interpol en de Verenigde Naties, en op zijn functie als hoofd van de afdeling Policy, Law & Ethics bij de Singularity University. Goodmans bestseller Future Crimes kreeg goede kritieken van The Financial Times, Ray Kurzweil en Peter Diamandis. Hierin laat Goodman zien hoe criminelen, bedrijven en overheden exponentionele technologiën tegen ons gebruiken. Goodman denkt dat we een aantal duidelijke stappen kunnen nemen om de controle over onze data te herwinnen en te ontkomen aan de exponentionele ontwikkelingen die zich nu voordoen.

ontdekt. Gemiddeld kost het 211 dagen om een besmetting te ontdekken. Er zitten nu dus slechteriken in het systeem waarvan we nog niets weten."

Het is belangrijk dat cyberaanvallen tijdig worden ontdekt, want de gevolgen kunnen ernstig zijn. "70% van de kleine en middelgrote bedrijven die gehackt worden, stopt er binnen een half jaar mee. En 62% van de cyberaanvallen is gericht op kleine en middelgrote bedrijven. Helaas is het maar in 6% van de gevallen de IT-afdeling die een hack ontdekt. 94 van de 100 keer gebeurt dat doordat klanten klagen of de politie voor de deur staat. Bedrijven zouden een open-source intelligenceprogramma moeten hebben, en iemand die verantwoordelijk is voor de veiligheid die criminelen begrijpt. Ze zouden hun eigen systemen moet proberen te hacken. En: als iets heel belangrijk is, zet het dan niet in de computer."

Vooruitgang overleven

Wat doen we verder als maatschappij? Hoe overleven we de vooruitgang? "Nu alles gedomineerd wordt door software, regeert computercode de wereld", zegt Goodman. "Een politieagent uit Amsterdam kan niet iemand arresteren in Moskou of New York, vanwege het Verdrag van Westfalen. Maar cybercriminelen kunnen al die regels negeren en worden steeds internationaler. We hebben een 21ste-eeuws probleem, en om het aan te pakken hebben we 19de-eeuwse instituties."
Bedrijven zullen deel moeten uitmaken van de oplossing, vindt Goodman. "Werkgevers zullen een mechanisme moeten creëren waarmee werknemers bedreigingen kunnen waarnemen en stoppen, en waarmee ze hun zorgen kunnen delen."
Verder moet er een wereldwijd back-upplan komen. "Als er ooit iets misgaat met alles waarbij computers een rol spelen – water, gas, auto's, vliegtuigen – dan kunnen we nergens op terugvallen. Onze 21ste-eeuwse wereld is een kaartenhuis. Het wordt tijd dat we deze existentiële bedreiging serieus gaan nemen. En ik denk dat we er iets op kunnen vinden."

"De 21ste eeuw kan fantastisch worden, maar we zullen er hard voor moeten werken."

"Onze 21ste-eeuwse wereld is een kaartenhuis. Het wordt tijd dat we deze existentiële bedreiging serieus gaan nemen. En ik denk dat we er iets op kunnen vinden."

Technologie kan geweldig zijn, wil Goodman maar zeggen. "De komende jaren trekt technologie twee miljard mensen uit de armoede. We gaan mensenlevens verlengen, kindersterfte verminderen en mensen opleiden die nog nooit een opleiding hebben gehad. Technologie kan ook misbruikt worden. De 21ste eeuw kan fantastisch worden, maar we zullen er hard voor moeten werken. Als we dat doen, ziet de toekomst er stralend uit. De mensheid heeft al vaker ongelooflijke dingen gedaan."