

# CODE ROOD

Tekst: Ramses Sloeserwij  
Met dank aan Richard van der Kraan & Maurits van den Heuvel  
Foto omslag: Susan Dammingsh  
Vormgeving: Studio Spade  
ISBN: 978-90-825499-6-6

Copyright © 2022, Red Angle en Communicatiereeks

Alle rechten voorbehouden. Niets uit deze uitgave mag worden verveelvoudigd, opgeslagen in een geautomatiseerd gegevensbestand, of openbaar gemaakt, in enige vorm of op enige wijze, hetzij elektronisch, mechanisch, door fotokopieën, opnamen, of enige andere manier, zonder voorafgaande schriftelijke toestemming van de rechthebbende.

Ramses Sloeserwij en Communicatiereeks hebben zich ingespannen om alle rechthebbenden van het geplaatste materiaal te achterhalen. De aard van het materiaal brengt evenwel met zich mee dat in sommige gevallen de identiteit of verblijfplaats van rechthebbenden in redelijkheid niet kan worden achterhaald.

Zij die menen rechten te kunnen doen gelden kunnen zich melden via de uitgever.

# VOORWOORD

7 mei 2021 kwam het bericht naar buiten dat het Texaanse oliebedrijf Colonial Pipeline geraakt was door een ransomware-aanval. De cybercriminelen vroegen losgeld in de vorm van cryptovaluta. Na het betalen van 4,4 miljoen dollar werd de digitale gijzeling op 12 mei opgeheven. Gevolg was wel een totale verstoring van het dagelijkse leven. Grote run op brandstof, ellenlange rijen bij tankstations en verhoogde brandstofprijzen. Kort daarvoor kwam ook het nieuws naar buiten dat Russische cybercriminelen wisten te infiltreren in de beheerssoftware van IT-bedrijf SolarWinds om daarmee een zogenaamde supply-chainaanval uit te kunnen voeren. Het gevolg hiervan was ongewenste toegang tot minstens 18.000 overheids- en particuliere netwerken, waaronder zelfs het Pentagon. Dit zijn slechts twee zeer recente voorbeelden, en we kunnen ervan uitgaan dat er meer en nog grotere cyberaanvallen zullen volgen. We moeten cyberaanvallen niet langer beschouwen als incidenten, want op de lange termijn is dat zeer gevaarlijk: cyberaanvallen raken het hart van onze maatschappij. Recent waarschuwde Huib Modderkolk er al voor in zijn boek *'Het is oorlog maar niemand die het ziet'*. En zoals Johan Cruijff het ooit al eens zei: *'Je ziet het pas als je het door hebt'*. Met andere woorden: als je er even meer aandacht aan besteedt, zie je een schrikbarende toename. Een toename waardoor we van lieverlede mogen spreken over een Code Rood-situatie. Het cyberdomein staat wat dat betreft figuurlijk in brand.

Wat is er aan de hand? Waardoor komt dat? Dit boek probeert hierop een antwoord te geven. Wat verzwakt ons cyberdomein en hoe kunnen we dat tegengaan? Welke cyberactoren zijn er, waardoor raken ze gemotiveerd en hoe gaan ze te werk? Om je te kunnen verdedigen, moet je weten wie je vijand is en welke strategie deze hanteert.

Internet heeft echt een volgende stap in de evolutie van de mens veroorzaakt. Naast de fysieke wereld ontstaat een totaal nieuwe wereld, een virtuele wereld: het cyberdomein. Een wereld die langzaam maar zeker een steeds grotere invloed gaat krijgen op de fysieke wereld. Kijk bijvoorbeeld naar de ontwikkelingen in China rond surveillancesystemen en het Social Credit System. Dit klinkt voor de Nederlander ver weg maar onze eigen coronamelder-app heeft al een eerste aanzet hiertoe gegeven. Trek deze lijn maar eens door naar de toekomst.

6.2.1 Voorgeschiedenis	51
6.2.2 Cybermotivatie	52
6.2.3 Cybereenheden	52
6.2.4 Cyberactiviteiten	56
6.2.5 Samenvatting	59
6.3 China	61
6.3.1 Voorgeschiedenis	63
6.3.2 Cybermotivatie	65
6.3.3 cybereenheden	66
6.3.4 Cyberactiviteiten	71
6.3.4.1 Cyber versus economie	72
6.3.4.2 Cyber versus Censuur	80
6.3.4.3 Cyber versus Imperialisme	85
6.3.5 Samenvatting	89
6.4 Rusland	91
6.4.1 Voorgeschiedenis	91
6.4.2 Cybermotivatie	92
6.4.3 Cybereenheden	94
6.4.4 Cyberactiviteiten	100
6.4.5 Samenvatting	109
6.5 Iran	111
6.5.1 Voorgeschiedenis	111
6.5.2 Cybermotivatie	112
6.5.3 Cybereenheden	112
6.5.4 Cyberactiviteiten	116
6.5.5 Samenvatting	120
6.6 Noord-Korea	121
6.6.1 Voorgeschiedenis	122
6.6.2 Cybermotivatie	122
6.6.3 Cybereenheden	124
6.6.4 Cyberactiviteiten	128
6.6.5 Samenvatting	136
7. Ontwikkeling Criminele Actoren	138
7.1 Carbanak Gang oftewel Crime of the Century	139
7.1.1 De infiltratie	139
7.1.2 Cashing	140
7.1.3 Geldvervoer	141
7.1.4 Het vervolg	141
7.1.5 Wie waren het?	144
7.1.6 Samenvatting	146
7.2 Fraude-industrie	147
7.2.1 Ransomware-industrie	147

# INHOUD

Voorwoord	v
Inhoud	vi
Opbouw boek	1
1. Inleiding	2
2. Code Rood samenvatting oorzaken	4
2.1 Technologische ontwikkelingen	6
2.2 Menselijke ontwikkelingen	7
2.3 Ontwikkelingen statelijke actoren	7
2.4 Ontwikkelingen criminele actoren	8
3. Technologische ontwikkelingen	9
3.1 Toename vergrijzing technologische footprint	10
3.2 Toename totale technologische footprint	11
3.2.1 Information Technology (IT)	11
3.2.2 Internet-of-Things (IoT)	12
3.2.3 Operational Technology (OT)	15
3.3 Toename totale kwetsbaarheid	16
3.3.1 The world of vulnerabilities	16
3.3.2 Toename aantal kwetsbaarheden	22
3.4 Toename complexiteit	23
3.4.1 Oplopende architectuurschuld	23
3.5 Samenvatting	24
4. Menselijke ontwikkelingen	26
4.1 Menselijke disruptie	26
4.2 Human legacy oftewel vasthouden aan oude gewoontes	28
4.3 Silver Bullet Syndrome	28
4.4 Compliance-denken	30
4.5 Security-fundamentalisme	32
4.6 Samenvatting	33
5. Maatschappelijke ontwikkelingen	35
5.1 Organisatorische disruptie	35
5.2 The End of the Free Internet	37
5.3 Privacy, delfstof van de 21e eeuw	38
5.4 Fysieke versus virtuele wereld	40
5.5 Old World versus New World	42
5.6 War of the Ecosystems	44
5.7 Samenvatting	45
6. Ontwikkeling Statelijke Actoren	47
6.1 Top-5 cyberlanden	48
6.2 Verenigde Staten	51

7.2.2 BEC-fraude/CEO-fraude	152
7.2.3 E-mailfraude	154
7.2.4 Samenvatting	156
7.3 Botnets	157
7.4 Free heavens	159
8. Maar wat kunnen we doen?	162
8.1 Security Governance	163
8.2 Basis op orde hebben en houden	164
8.2.1 Zorg voor duidelijk eigenaarschap	164
8.2.2 Zorg voor duidelijke classificatie	165
8.2.3 Zorg voor aantoonbaarheid	165
8.2.4 Zorg voor scheiding (segregation) op basis van het risico	166
8.2.5 Zorg voor doelbinding	167
8.2.6 Zorg voor robuustheid (hardening)	167
8.2.7 Zorg voor een stringent backup-regime	169
8.2.8 Zorg voor wenselijk dataverkeer	170
8.2.9 Zorg voor de juiste afscherming	171
8.3 Security-architectuur	172
8.3.1 Zero Trust model	173
8.3.2 Reducing the Attack Surface	175
8.4 Security by Design	177
8.5 Security Monitoring	179
8.5.1 Security Tests	179
8.5.2 Anomaly Detection	181
8.6 Identity & Access Management	183
8.6.1 Public Key Infrastructure	185
8.7 Risicobewust handelen	187
8.8 The Art of Attribution	190
8.9 Cyber Kill Chain	193
8.10 Security Intelligence	196
8.10.1 Vulnerability Management	196
8.10.2 Red & Blue Teaming	197
8.11 Toekomstige ontwikkelingen	199
8.11.1 Wetgeving rond cyber	199
8.11.2 Minister van Digitale Zaken	200
8.11.3 Privacy-ontwikkelingen	200
8.11.4 Paradigm shift	201
Begrippenlijst	203
Bronnen	205
Figuren en tabellen	210

## 2. CODE ROOD

### SAMENVATTING OORZAKEN

Het cyberdomein is nog jong en daarom realiseert niet iedereen zich hoe gevaarlijk dit domein is. Zo is bijvoorbeeld op Hackmageddon.com — een website die alle cyberaanvallen registreert en deze op alle manieren statistisch weergeeft— te zien dat het werkelijke aantal cyberaanvallen nog altijd jaarlijks toeneemt. Van 1337 aanvallen in 2018 naar 2539 in 2021 — haast een verdubbeling in enkele jaren. En deze trend zal zeker verder doorzetten.

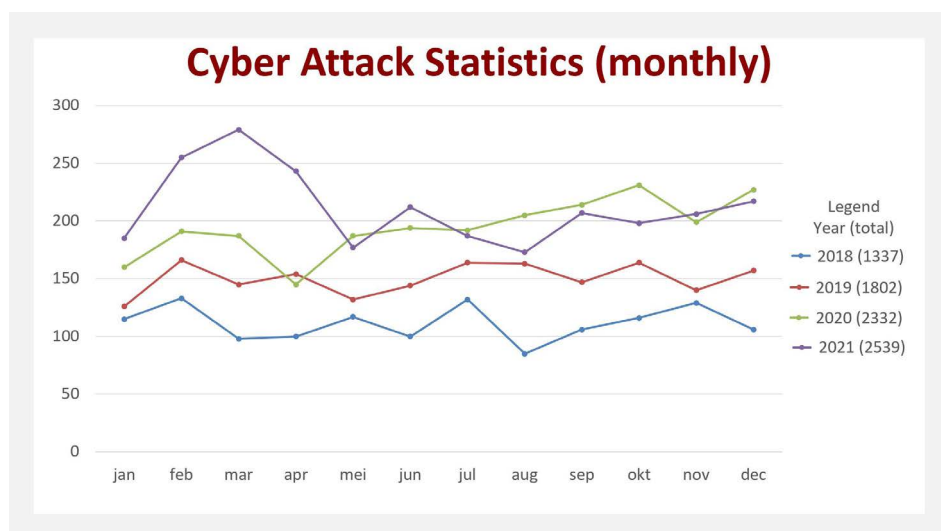


Fig. 2: Aantal cyberaanvallen tussen 2018 en 2021.

Deze toename blijkt niet alleen uit het aantal cyberaanvallen maar ook uit de jaarlijkse financiële schade die het veroorzaakt. Want als we kijken naar de totale schade die in de Verenigde Staten bij het Internet Crime Compliant Center (IC3) is geregistreerd, dan zien we dat het bedrag aan schade van 2001 tot 2020 een nagenoeg identieke verdubbeling toont.

In de laatst gerapporteerde periode bedroeg het verlies aan cybercriminaliteit 4,2 miljard dollar, tegen 1 miljard dollar in 2015. Goed, dit zijn cijfers uit de Verenigde Staten, maar het is aannemelijk dat deze stijging ook in de rest van de wereld te zien zal zijn. Overigens geldt dit niet alleen voor westerse welvarende landen, want cybercriminelen verdienen evengoed aan minder welvarende landen.

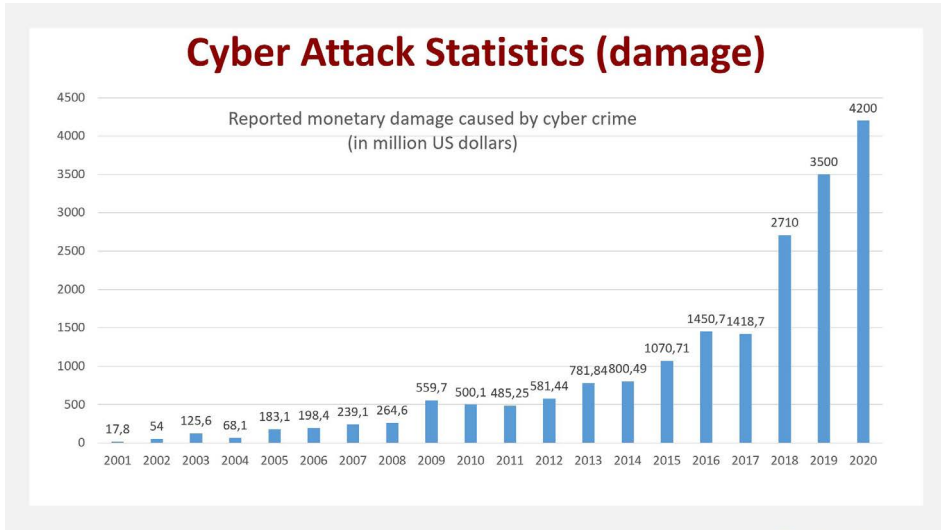


Fig. 3: Financiële schade in de VS door cybercriminaliteit.

Als we naar het aantal buitgemaakte datarecords kijken, gaan helemaal alle alarmbellen af. Zo laat een studie van Selfkey.org zien — dat is een organisatie die zich inzet voor identiteitsbeveiliging — dat er elke twee seconden een nieuw persoon slachtoffer is van identiteitsdiefstal. Ook deze studie richt zich weer alleen op de Verenigde Staten maar de uitkomsten mogen natuurlijk ook de rest van de wereld zorgen baren.

Deze criminaliteitstoename is niet enkel toe te schrijven aan het uitdijende cyberdomein. Er zijn hier meerdere ontwikkelingen debet aan, zoals ontwikkelingen op technologisch, menselijk en maatschappelijk gebied. Denk aan de combinatie van vergrijzing, digibetisme, oude gewoontes, geopolitieke spanningen en de lage pakkans van cybercriminelen. Deze oorzaken versterken elkaar, waardoor er een synergetisch effect ontstaat. Parallel daaraan zie je dat statelijke actoren zich steeds offensiever opstellen en misbruik maken van de nieuwe kansen en mogelijkheden uit het cyberdomein. Daarnaast worden cybercriminelen steeds professioneler en volhardender. Met andere woorden: het geheel wordt groter en kwetsbaarder terwijl aan de andere kant de dreiging groter wordt.



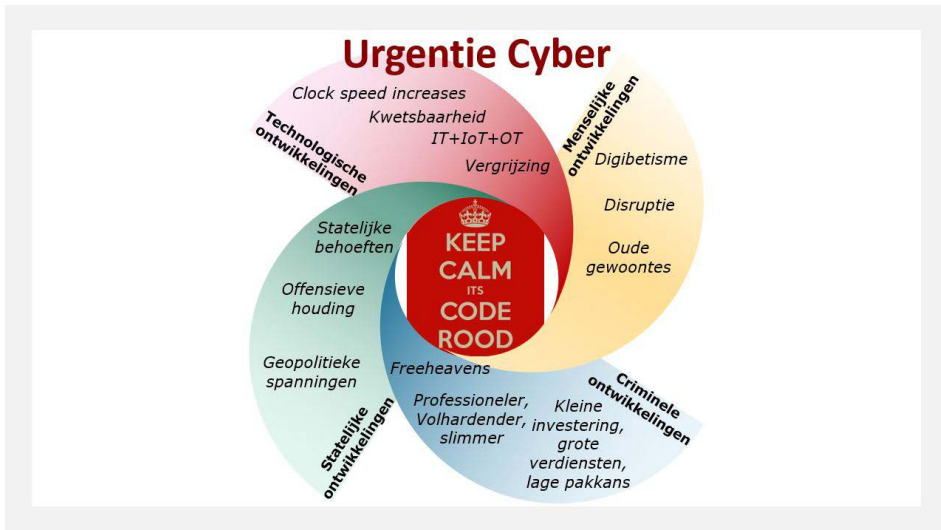


Fig. 4: Synergie tussen verschillende ontwikkelingen leidt tot een versnelde cyberdreiging.

## 2.1 Technologische ontwikkelingen

### Technologische footprint veroudert steeds sneller

Technologische ontwikkelingen gaan steeds sneller — haast exponentieel. Hierdoor ontstaat een Technology Push-markt, waardoor chips steeds sneller werken (de *clock speed increases*) de levenscyclus van producten steeds korter wordt en de veroudering, ook wel vergrijzing genoemd, sneller toeneemt. Als direct logisch gevolg daarvan neemt de kwetsbaarheid ook toe.

### Technologische footprint wordt steeds groter (IT + IoT + OT)

Steeds meer productonderdelen worden uitgerust met internettechnologie en deze worden vervolgens op het internet aangesloten. Naast een groeiend Information Technology (IT)-park, groeit ook het Internet-of-Things (IoT), maar worden ook steeds meer Operational Technology (OT)-componenten op het internet aangesloten. Hierdoor groeit onze totale technologische footprint explosief. Daarnaast neemt het aantal onveilige componenten zoals IoT- en OT-componenten ook steeds meer toe. Gevolg hiervan is dat we steeds kwetsbaarder worden, onze *attack surface* wordt vergroot.

### Aantal zwakheden (vulnerabilities) neemt jaarlijks toe

Zwakheden of *vulnerabilities* zijn inherent aan geprogrammeerde softwareregels. Ondanks dat gevonden zwakheden worden verholpen — dankzij *security patches* — introduceren we ook steeds weer nieuwe kwetsbaarheden.

## **Complexiteit van de totale technologische footprint neemt verder toe**

Organisaties maken in toenemende mate gebruik van technologische diensten van derden, in diverse uiteenlopende vormen — denk aan *On-premise, private/public/hybrid Cloud, PaaS/SaaS* — wat de totale technologische footprint diffuus maakt.

## **2.2 Menselijke ontwikkelingen**

### **Toenemend digibetisme**

Naarmate mensen ouder worden, hebben ze steeds meer moeite om met de digitale wereld om te kunnen gaan; er ontstaat digibetisme.

### **Steeds groter wordende disruptie**

Technologie ontwikkelt zich haast exponentieel maar het menselijke aanpassingsvermogen volgt niet eenzelfde ontwikkeling, deze is eerder lineair. Niet alleen individuen, maar zelfs hele organisaties kunnen en zullen dat tempo niet meer bijhouden. Er ontstaat een ontwrichting of disruptie.

### **Vasthouden aan oude gewoontes/oud denken**

Mensen maar ook organisaties houden zich graag vast aan oude gewoontes. Immers: het verleden heeft aangetoond dat deze werken. Het vermogen om zich continu aan te passen is slechts beperkt.

### **Beperkt lerend vermogen**

De wil om te leren van fouten van andere organisaties is maar zeer beperkt. Criminelen hanteren vaak een vast patroon in hun aanval. Verandering is niet noodzakelijk omdat andere organisaties hier toch niet van leren.

### **Security-fundamentalisme**

Security moet business mogelijk maken maar door de tijd heen worden security-functionarissen zodanig geconditioneerd dat zij niet meer denken in mogelijkheden. Elk risico roept weerstand op waardoor ze houvast vinden in 'kan niet, mag niet'.

## **2.3 Ontwikkelingen statelijke actoren**

Het cyberdomein wordt door vrijwel alle krijgsmachten beschouwd als het vijfde operationele domein. Diverse landen, en dan niet alleen de 'usual suspects', maken er maar al te graag handig gebruik van om uiteenlopende redenen. Een aantal daarvan is bovengemiddeld actief in dit domein en haalt geregeld op zeer negatieve wijze het nieuws, waaronder: