Themarapportage cyberdreigingen

Deze themarapportage is onderdeel van de Rijksbrede Risicoanalyse Nationale Veiligheid

Analistennetwerk Nationale Veiligheid

Themarapportage cyberdreigingen

Deze themarapportage is onderdeel van de Rijksbrede Risicoanalyse Nationale Veiligheid

Analistennetwerk Nationale Veiligheid

Colofon

Deze themarapportage is gemaakt door het Analistennetwerk Nationale Veiligheid
in opdracht van de NCTV.

Het Rijksinstituut voor Volksgezondheid en Milieu (RIVM)
Nederlandse Organisatie voor toegepast-natuur-wetenschappelijk onderzoek (TNO)
Stichting Nederlands Instituut voor Internationale Betrekkingen `Clingendael' (Clingendael)
SEO Economisch Onderzoek (SEO)
Algemene Inlichtingen- en Veiligheidsdienst (AIVD)
Militaire Inlichtingen- en Veiligheidsdienst (MIVD)
Wetenschappelijk Onderzoek- en Documentatiecentrum (WODC)

Contact: ir. L. Gooijer (leendert.gooijer@rivm.nl)

Inhoudsopgave

1. Inleiding

Deze rapportage is onderdeel van de Rijksbrede Risicoanalyse (RbRa), uitgevoerd door het Analistennetwerk Nationale Veiligheid (ANV). Het doel van de RbRa is het in kaart brengen van verschillende typen dreigingen voor de nationale veiligheid van het Koninkrijk der Nederlanden. Hiertoe worden mogelijke dreigingen niet alleen geïdentificeerd, maar wordt ook een inschatting gemaakt van waarschijnlijkheid en mogelijke gevolgen (het 'risico'). Deze inschatting vindt plaats aan de hand van door het ANV opgestelde scenario's. De dreigingen in kwestie zijn verdeeld over negen verschillende inhoudelijke dreigingsthema's, elk onderverdeeld in meerdere categorieën met daarin één of meerdere scenario's. Voor elk van de thema's wordt een themarapport opgesteld. De themarapporten dienen als basis voor het hoofdrapport van de RbRa. De verschillende thema's en daaronder vallende categorieën worden in dit eindproduct gezamenlijk beschouwd aan de hand van de zes nationale veiligheidsbelangen. Zodoende wordt een overzicht gegeven van de belangrijkste risico's voor de nationale veiligheid.

Deze rapportage bevat de door het ANV uitgevoerde analyses voor het thema cyberdreigingen. Onder dit thema vallen drie dreigingscategorieën, met verschillende scenario's die de dreigingen illustreren.

Het themarapport cyberdreigingen bestaat uit een aantal onderdelen. Hoofdstuk twee geeft een algemene introductie tot het thema, de drie in deze rapportage opgenomen dreigingscategorieën en de door het ANV gehanteerde werkwijze. Per dreigingscategorie zullen ontwikkelingen, een overzicht van actoren en factoren, de scenario's inclusief impact- en waarschijnlijkheids-beoordeling en een dreigingscategorie beschouwing worden behandeld. Hoofdstuk drie gaat over de dreigingscategorie verstoring functioneren Internet, hoofdstuk vier behandelt verstoring cyber-fysieke systemen en hoofdstuk vijf gaat over cybercrime. Hoofdstuk zes zal een tweetal sluimerende dreigingen behandelen. Dit zijn ontwikkelingen die binnen de tijdshorizon van 5 jaar nog geen concrete dreiging voor de nationale veiligheid vormen, maar die zich naar verwachting wel als zodanig zullen ontwikkelen als de trend zich zal doorzetten. Hoofdstuk zeven bevat een algemene slotbeschouwing voor het thema als geheel.

2. Achtergrond en dreigingscategorieën

2.1 Dreigingscategorieën

Digitale systemen raken steeds meer verweven in onze samenleving en een duidelijk onderscheid tussen het fysieke of digitale domein is eigenlijk niet meer te maken. Als het gaat om dreigingen voor de nationale veiligheid kunnen digitale systemen zowel middel als doelwit zijn van aanvallen en ook niet-moedwillige verstoringen van digitale systemen kunnen veroorzaakt worden door uiteenlopende oorzaken zoals een natuurramp, een ongeval of door technische of menselijke fouten.
Veel van deze oorzaken (en gevolgen) worden geadresseerd in andere thema's van de Rijksbrede Risicoanalyse en 'cyber' is dus ook een onderwerp dat veel samenhang kent met andere onderwerpen. In verschillende andere themarapportages worden dan ook cyber-gerelateerde dreigingen en ontwikkelingen benoemd, bijvoorbeeld binnen het thema bedreiging vitale infrastructuur (er zijn immers ook digitale processen die als vitaal zijn bestempeld), maar ook als onderdeel van een hybride dreiging, spionage of binnen het thema economische dreigingen.

In dit thema cyberdreigingen worden typen dreigingen samengebracht die specifiek voortkomen uit de digitalisering van de samenleving en dus niet een 'digitale variant' van een fenomeen dat in andere thema's al aan bod komt (dit is bijvoorbeeld de reden dat cyberspionage niet binnen dit thema is opgenomen, maar als onderdeel van de dreigingscategorie spionage binnen het thema ongewenste inmenging en ondermijning democratische rechtstaat).
We maken binnen dit thema onderscheid tussen drie dreigingscategorieën:

- Verstoring functioneren Internet
- Verstoring cyber-fysieke systemen
- Cybercrime

In de eerste dreigingscategorie, verstoring functioneren internet, staan gebeurtenissen centraal die ervoor kunnen zorgen dat de toegang tot of werking van het Internet en Internetdiensten belemmerd wordt. De tweede dreigingscategorie, verstoring cyber-fysieke systemen, richt zich op dreigingen die ontstaan door de toenemende digitalisering van industriële en andere fysieke processen, vaak via zogenoemde Industriële Controle Systemen. In de laatste dreigingscategorie, cybercrime, gaan we in op de dreiging voor de nationale veiligheid van vormen van criminaliteit die door de digitalisering van de samenleving ontstaan en mogelijk gemaakt worden.

Digitale systemen en netwerken zijn in sterke mate met elkaar verbonden en maken vaak gebruik van hard- en software en diensten van dezelfde leveranciers. Niet voor niets wordt veel aandacht besteed aan cyberincidenten die vanuit de IT *supply chain* veroorzaakt worden.[1] Dit kan gezien worden als een eigen onderwerp en verdient ook een plek in een analyse van cyberdreigingen, maar het heeft meer te maken met de manier waarop een incident zich voltrekt en is dus één van de factoren die bij het analyseren van dreigingen in de genoemde categorieën aandacht moet krijgen.

[1] Voor een definitie, taxonomie en analyse van it supply chain aanvallen, zie ifigeneia lella, marianthi theocharidou, eleni tsekmezoglou, apostolos malatras, sebastian garcia, veronica valeros, ed., Enisa threat landscape for supply chain attacks (european union agency for cybersecurity, 2021), https://www.Enisa.Europa.Eu/publications/threat-landscape-for-supply-chain-attacks.

2.2 Aanpak

Dit themarapport bevat voor elk van de drie dreigingscategorieën een overzicht van relevante ontwikkelingen en een nadere analyse van de dreiging behorende tot de categorie in kwestie. Deze analyse is vormgegeven aan de hand van scenario's. Voor elke categorie zijn één of meerdere scenario's uitgewerkt ter illustratie van hoe de dreiging zich mogelijk kan manifesteren. In totaal zijn er voor het gehele thema vijf reguliere scenario's en één wild-card-scenario uitgewerkt in de vorm van een verhaallijn. De scenario's zijn tot stand gekomen in samenspraak met deskundigen behorende tot organisaties verbonden aan het ANV. De scenario's zijn nadrukkelijk bedoeld om de fenomenen verstoring functioneren Internet, verstoring cyber-fysieke systemen en cybercrime te illustreren en zijn niet uitputtend. Binnen de RbRa wordt geen volledigheid nagestreefd met betrekking tot de opgenomen scenario's.

Voor elk van de reguliere scenario's zijn op basis van *expert judgement* zowel de waarschijnlijkheid als de mogelijke gevolgen in kaart gebracht aan de hand van de door het ANV ontwikkelde methodiek nationale veiligheid.

Voor het wild-card-scenario is samen met experts een eerste (kwalitatieve) indicatie gegeven van de mogelijke impact op de nationale veiligheid (zie voor een korte uitleg van een wild card paragraaf 2.2.2). In Bijlage 1 staat een overzicht van de organisaties die hebben deelgenomen aan de expertsessies voor dit thema.

2.2.1 Methodiek nationale veiligheid

Binnen deze methodiek wordt gekeken of en in welke mate een bepaalde gebeurtenis de zes nationale veiligheidsbelangen raakt. De nationale veiligheid is in het geding als één of meer van de zes nationale veiligheidsbelangen dusdanig worden bedreigd dat er sprake is van (potentiële) maatschappelijke ontwrichting. [2] De zes belangen zijn elk opgesplitst in één of meerdere meetbare impactcriteria die helpen bij het in kaart brengen van een mogelijke aantasting. Onderstaande tabel geeft een kort overzicht van alle belangen en criteria. Een uitgebreide uitleg voor elk van deze onderdelen bevindt zich in de door het ANV opgestelde leidraad risicobeoordeling. [3]

Tabel 1 Belangen en impactcriteria behorende tot de methodiek nationale veiligheid

Belang	Impactcriteria
1. Territoriale veiligheid	1.1 Aantasting van de integriteit van het grondgebied van het Koninkrijk der Nederlanden
	1.2 Aantasting van de integriteit van de internationale positie van het Koninkrijk der Nederlanden
	1.3 Aantasting van de integriteit van de digitale ruimte
	1.4 Aantasting van de integriteit van het bondgenootschappelijk grondgebied
2. Fysieke veiligheid	2.1 Doden
	2.2 Ernstig gewonden en chronisch zieken
	2.3 Gebrek aan primaire levensbehoeften
3. Economische veiligheid	3.1 Kosten
	3.2 Aantasting van de vitaliteit van de economie van het Koninkrijk der Nederlanden
4. Ecologische veiligheid	4.1 Langdurige aantasting van het milieu en de natuur

[2] ANV, Leidraad Risicobeoordeling Rijksbrede Risicoanalyse Nationale Veiligheid (Bilthoven: RIVM, 2020), https://www.rivm.nl/onderwerpen/nationale-veiligheid.

[3] Idem.

Belang	Impactcriteria
5. Sociale en politieke stabiliteit	5.1 Verstoring van het dagelijkse leven
	5.2 Aantasting van de democratische rechtstaat
	5.3 Sociaal-maatschappelijke impact
6. Internationale rechtsorde	6.1 Aantasting van de normen van staatssoevereiniteit, vreedzame co-existentie en vreedzame geschillenbeslechting
	6.2 Aantasting van de werking, legitimiteit dan wel naleving van de internationale verdragen en normen inzake de rechten van de mens
	6.3 Aantasting van een op regels gebaseerd internationaal financieel-economisch bestel
	6.4 Aantasting van de effectiviteit, legitimiteit van multilaterale instituties
	6.5 Instabiliteit van staten grenzend aan het Koninkrijk der Nederlanden en in de directe omgeving van de Europese Unie

Voor het geven van een oordeel over de precieze omvang van de gevolgen van een scenario, wordt aan elk van de criteria een impactscore toegekend, namelijk: niet van toepassing, beperkt (A), aanzienlijk (B), ernstig (C), zeer ernstig (D) of catastrofaal (E). Deze classificering is gebaseerd op een logaritmische schaal. Voor criterium 2.1 (aantal doden) betekent dit bijvoorbeeld dat een beperkte score staat voor 0-10 doden, een aanzienlijke score voor 10-100 doden, et cetera. Eenzelfde redenatie wordt gehanteerd voor criterium 3.1 (kosten). Er is sprake van maatschappelijke ontwrichting als één of meer van de belangen ernstig (klasse C) of hoger wordt aangetast.

Tabel 2 Voorbeeld van verschillende klassen van gevolg binnen de methodiek nationale veiligheid

Klasse van gevolgen	Voorbeeld criterium: Aantal doden (2.1)	Voorbeeld criterium: kosten (3.1)
A. Beperkt	Minder dan 10	< 50 miljoen euro
B. Aanzienlijk	10 tot 100	< 500 miljoen euro
C. Ernstig	100 tot 1000	< 5 miljard euro
D. Zeer ernstig	1000 tot 10.000	< 50 miljard euro
E. Catastrofaal	Meer dan 10.000	> 50 miljard euro

In tegenstelling tot de bovenstaande criteria 2.1 en 3.1, zijn sommige criteria niet uit te drukken in een absoluut aantal. Een voor dit thema relevant voorbeeld is criterium 1.3, aantasting van de integriteit van de digitale ruime. Hier wordt gekeken of er sprake is van een schending (ongewenste toegang verkregen tot IT netwerken en informatiesystemen van Nederlandse gebruikers) van controle/zeggenschap over de digitale ruimte van het Koninkrijk der Nederlanden. De ernst van de impact wordt niet bepaald door de daadwerkelijke gevolgen van de schending, maar in eerste instantie door het type organisatie waarvan de integriteit van IT netwerken of informatiesystemen geschonden zijn:

- Vitale aanbieders;
- Rijksoverheid, digitale dienstverleners, topsectoren of kennisinstellingen;
- Overige organisaties.

Vervolgens wordt gekeken naar het motief van de actor die de integriteit geschonden heeft. Indien dit een ideologisch of politiek motief betreft wordt de impact als zwaarder beoordeeld. Ook de omvang van de schending (worden er meerdere organisaties getroffen, hoe wijdverspreid is de schending?) wordt meegewogen bij de impactscore. Tenslotte wordt de impact eventueel weer verlaagd indien er sprake is van grip op de duur van de schending (de toegang is weer ontzegd).

Voor elk van de binnen dit thema beoordeelde scenario's zal aan de hand van een scorekaart per criterium worden weergegeven van welke orde grootte de verwachte gevolgen zijn.

Binnen de methodiek wordt niet alleen gekeken naar de gevolgen van gebeurtenissen, maar ook naar de waarschijnlijkheid van voorkomen. Voor het bepalen van de waarschijnlijkheid, wordt gekeken naar de kans van voorkomen binnen het moment van analyse (eerste kwartaal 2022) en vijf jaar. Deze kans wordt afhankelijk van het type gebeurtenis kwalitatief of kwantitatief weergegeven op een vijfpuntschaal van zeer onwaarschijnlijk tot zeer waarschijnlijk. Voor moedwillige gebeurtenissen zoals die omschreven binnen dit themarapport, wordt een kwalitatieve schaal gehanteerd.

Ook de ingeschatte waarschijnlijkheid zal voor elk van de tien scenario's worden weergegeven in de eerder genoemde scorekaart. Om te helpen bij de uiteindelijke vergelijking van alle scenario's, bevat hoofdstuk zeven een risicodiagram met een overzicht van de scenario's geplot langs de assen waarschijnlijkheid en totale gevolgen.

Tabel 3 Klassen van waarschijnlijkheid binnen de methodiek nationale veiligheid

Klasse van waarschijnlijkheid	Kwalitatieve omschrijving van de dreiging
A. Zeer onwaarschijnlijk	Geen concrete aanwijzingen en het scenario wordt niet voorstelbaar geacht
B. Onwaarschijnlijk	Geen concrete aanwijzingen, maar het scenario wordt enigszins voorstelbaar geacht
C. Enigszins waarschijnlijk	Geen concrete aanwijzingen, maar het scenario is voorstelbaar
D. Waarschijnlijk	Het scenario wordt zeer voorstelbaar geacht; er zijn enige aanwijzingen dat het scenario zich daadwerkelijk zal voordoen,
E. Zeer waarschijnlijk	Concrete aanwijzingen dat het scenario geëffectueerd zou kunnen worden

2.2.2 Bouwstenen, wild cards & sluimerende dreigingen

Ten behoeve van het identificeren en uitwerken van de scenario's is gebruik gemaakt van 'bouwstenen'. Bouwstenen zijn een overzicht van de voor een dreigingscategorie relevante actoren en factoren. Door actoren en factoren te combineren kunnen meerdere situaties ofwel scenario's worden gecreëerd. Uiteraard zullen verschillende combinaties leiden tot verschillende scenario's met wisselende uitkomsten. De bouwstenen helpen om in één oogopslag duidelijk te maken wat wel en wat niet is meegenomen in het scenario en dienen als referentiekader voor de uiteindelijke verhaallijn. De in deze rapportage opgenomen scenario's betreffen enkele voorbeelden van hoe de dreiging behorende tot één van de drie categorieën zich kan manifesteren. Ze zijn nadrukkelijk niet uitputtend, maar streven ernaar een zo goed mogelijke afspiegeling te zijn van relevante actoren en factoren.

Naast de op bouwstenen gebaseerde scenario's, wordt er binnen dit thema ook een wild-card-scenario beschouwd met betrekking tot de sabotage van het *Domain Name System Security Extensions* protocol. Een wild card is een scenario met een relatief lage waarschijnlijkheid en een hoge impact of een grote mate van onzekerheid ten opzichte van de scenario's die op de bouwstenen zijn gebaseerd.

Tot slot worden er binnen dit thema ook twee sluimerende dreigingen beschouwd. Deze beschouwing betreft een bepaalde trend of ontwikkeling waarbij er niet alleen een inhoudelijke uiteenzetting plaatsvindt, maar er ook (per belang en op hoofdlijnen) een indicatie wordt gegevenvan mogelijke gevolgen.

2.2.3 Overzicht van ontwikkelingen

Voor het overzicht van relevante ontwikkelingen is geput uit verschillende openbare rapporten, aangevuld met de kennis van aan het ANV verbonden organisaties.

2.2.4 Vitale processen

Binnen de RbRa is er eveneens aandacht voor hoe verschillende dreigingen de voor de Nederlandse maatschappij vitale processen kunnen aantasten, onder andere in het dreigingsthema bedreiging vitale infrastructuur. Ook binnen de afzonderlijke themarapporten komen de mogelijke gevolgen voor vitale processen als de drinkwatervoorziening, de olievoorziening en de scheepvaartafwikkeling naar voren. [4] De wijze waarop verschilt echter per thema. Binnen dit thema cyberdreigingen wordt per scenario kort stilgestaan bij de impact op de vitale processen, daar waar relevant.

[4] Zie voor een compleet en actueel overzicht : "Overzicht vitale processen," NCTV (2022), https://www.nctv.nl/onderwerpen/vitale-infrastructuur/overzicht-vitale-processen.

3. Dreigingscategorie verstoring functioneren internet

Het gebruik van Internet en Internetdiensten in onze samenleving neemt alleen maar verder toe, waardoor het van belang is om zicht te houden op gebeurtenissen die het functioneren van het Internet kunnen verstoren evenals de potentiële gevolgen van dit type gebeurtenissen in de samenleving. De toenemende verwevenheid van digitale en fysieke processen in de samenleving zorgt ervoor dat verstoring van het functioneren van het Internet potentieel een maatschappij ontwrichtend effect heeft. [5]

Deze dreigingscategorie richt zich met name op de beschikbaarheid van het internet en internetdiensten. Het gaat hierbij om gebeurtenissen die ervoor zorgen dat het functioneren wordt aangetast. In veel gevallen gaat het om verstoringen van de beschikbaarheid, maar ook de vertrouwelijkheid of integriteit van de elementen die een rol spelen bij het functioneren van het internet en internetdiensten kunnen het functioneren aantasten. Er zijn nauwe raakvlakken met het dreigingsthema bedreiging vitale infrastructuur; internet en internettoegang is immers een vitaal proces.

De dreigingen die in deze categorie worden geanalyseerd zijn gerelateerd aan de manier waarop internet en internetdiensten zijn ingericht en de belangrijke (technische) elementen die een rol spelen bij het functioneren van het internet. Hiervoor wordt gebruik gemaakt van een ANV verkenning uit 2018. [6] In deze verkenning is gekeken naar de belangrijke elementen van het Internet, relevante kwetsbaarheden van deze elementen en gevolgen van de aantasting van deze elementen voor het functioneren van het Internet. Een van de belangrijkste inzichten uit de genoemde verkenning is dat de manier waarop het internet en de onderliggende elementen functioneren behoorlijk robuust is. Hoewel het zeker niet uit te sluiten is, zijn er relatief weinig situaties denkbaar waarbij het functioneren van het internet op zeer grote schaal en langdurig verstoord raken.

Dit beeld wordt ook bevestigd als we kijken naar recente voorbeelden van verstoringen van internet en internetdiensten. [7] Ernstige verstoringen komen voor, maar blijven vaak toch relatief beperkt tot een deel van de internetdiensten of gebruikers en ook is de duur van een verstoring vaak relatief kort. Dit hangt onder andere samen met de architectuur van het internet, maar ook met de grote (economische) belangen van dienstverleners om de betrouwbaarheid van hun diensten hoog te houden.

Tegelijkertijd worden de netwerken, systemen en diensten en de manier waarop deze een rol spelen in de samenleving steeds complexer en is het landschap continu in ontwikkeling. Dat zorgt ervoor dat de impact van verstoringen van internetdiensten op de samenleving onvoorspelbaar kunnen zijn en dat lastig is om hier goed grip op te krijgen en houden, zowel voor de dienstverleners als gebruikers van internet en internetdiensten.

3.1 Relevante ontwikkelingen

Content- en Cloud Service Providers steeds dominanter in het internet infrastructuur ecosysteem

De internet infrastructuur is continu in ontwikkeling en ook de positie van spelers in het ecosysteem evolueert. Historisch gezien is het altijd zo geweest dat de partijen

5 NCTV, *Cybersecuritybeeld Nederland* (CSBN) 2021 (Den Haag: 2021), 33, https://www.nctv.nl/documenten/publicaties/2021/06/28/cybersecuritybeeld-nederland-2021.

6 Theo van Ruijven, Hanneke Duijnhoven, Benno Overeinder, Jaap Akkerhuis, "ANV Verkenning t.b.v. de risicocategorie Aantasten functioneren Internet," *DHW-NO-TNO 2018 R10331* (Den Haag: TNO/NLnet Labs, 2018).

7 Maria Korolov en Alex Korolov, "Top 10 outages of 2021," Network World (31 januari 2022), https://www.networkworld.com/article/3648352/top-10-outages-of-2021.html.

die veel commerciële belangen hebben ook bepalen hoe het internet transformeert.

Recent is een verschuiving te zien waarbij *content- en cloud service providers* (CSP) steeds meer de dominante partijen worden en in toenemende mate wereldwijde private netwerken creëren, waardoor de positie van het publieke, open internet onder druk komt te staan. Veel cloudverkeer wordt in toenemende mate intern, door de grote CSPs volledig buiten het publieke open internet om afgehandeld. Dit levert met name voor de overheid een spanningsveld op: het hebben van een directe, eigen connectie naar de CSP is goed voor de robuustheid en veiligheid van de data en systemen van een gebruiker. Als het verkeer tussen organisaties echter volledig via de cloud verloopt dan is dat weliswaar robuust, maar is er geen enkele controle meer op. De kernwaarden van het open internet [8] worden dan ook steeds minder relevant en de overheid verliest controle. [9]

BGP (Border Gateway Protocol) is robuuster geworden

De ontwikkeling van het RPKI protocol [10] dat de afgelopen jaren veel aandacht heeft gekregen zorgt er voor dat *BGP Hijacking* minder makkelijk wordt voor kwaadwillenden. Het RPKI protocol is een vertrouwensdienst en fungeert als een digitale handtekening voor BGP routering. Het risico is nog niet verdwenen omdat de *uptake* van RPKI nog geen 100% is, maar is wel een stuk kleiner geworden. [11] Ook het MANRS [12] manifest draagt bij aan een robuuster BGP doordat dit het toepassen van actuele *best practices* op het gebied van *security* en *resilience* van het internet routing systeem stimuleert. [13]

Het BGP is nog altijd een van de belangrijkste elementen voor het functioneren van het Internet. Hoewel het strikt genomen geen storing van het BGP betrof, toont de Facebook storing van oktober 2021 [14] wel de belangrijke rol van dit protocol aan. Door de interne misconfiguratie werden de systemen van Facebook in feite ontkoppeld van het Internet en daarmee niet beschikbaar voor gebruikers wereldwijd.

DNS (Domain Name System) is nog altijd belangrijk én relatief robuust

Ook DNS blijft een van de belangrijkste elementen voor het goed functioneren van het internet, en tegelijkertijd is DNS bewezen robuust. Echt grootschalige verstoring van DNS is nauwelijks voorstelbaar, hoewel de verregaande concentratie van DNS dienstverlening bij een paar grote partijen de impact van een eventuele ernstige storing bij één van deze dienstverleners wel potentieel groter maakt. Door de welbekende DDoS aanval op DNS provider Dyn (2016) [15] werd duidelijk dat veel gebruikers afhankelijk waren van één DNS provider. Recent onderzoek [16] laat zien dat nog altijd veel organisaties geen redundantie voor DNS diensten hebben ingebouwd. Bovendien lijkt de markt zich nog altijd verder te concentreren, waardoor een storing bij één van de grote DNS providers een groot effect op de beschikbaarheid van diensten wereldwijd kan hebben.

Centrale positie van de Nederlandse internetinfrastructuur lijkt af te nemen

Het landschap van zeekabels verandert elk jaar drastisch, er komen veel kabels bij. Op dit moment lijkt Nederland haar centrale positie te verliezen waardoor de rol van Nederland en de Amsterdamse Internet Exchange (AMS-IX) in het Internetlandschap kleiner wordt. [17]

8 Internet Society, "Internet Invariants: What Really Matters," Public Policy Brief (26 september 2016), https://www.internetsociety.org/wp-content/uploads/2017/09/ISOC-PolicyBrief-InternetInvariants-20160926-nb.pdf.

9 J. Bosman, B.M.M. Gijsen, Evolution of Internet interconnection: Opinion paper, (Den Haag: TNO, 2020), http://resolver.tudelft.nl/uuid:38f93a1c-6e20-413d-a7fd-cc6919a7e348.

10 Resource Public Key Infrastructure, zie "RPKI documentation," RPKI, geraadpleegd op 10 juni 2022, https://rpki.readthedocs.io/en/latest/.

11 D. McPherson, "Routing Without Rumor. Securing the Internet's Routing System," in New Conditions and Constellations in Cyber, Cyberstability Paper Series, ed. A. Klimberg (Den Haag: The Hague Centre for Strategic Studies, 2021): 77-91, https://cyberstability.org/wp-content/uploads/2021/12/Cyberstability-Paper-Series.pdf.

12 Mutually Agreed Norms for Routing Security.

13 Adrian Wan, "ISPs Should Strongly Consider MANRS to Fight Cybercrime: World Economic Forum Report," MANRS (23 januari 2020), https://www.manrs.org/2020/01/isps-should-strongly-consider-manrs-to-fight-cybercrime-wef-report/.

14 Celso Martinho, Tom Strickx, "Understanding How Facebook Disappeared from the Internet," Cloudflare (4 oktober 2021), https://blog.cloudflare.com/october-2021-facebook-outage/; Santosh Janardhan, "Update about the October 4th outage," Engineering at Meta (4 oktober 2021), https://engineering.fb.com/2021/10/04/networking-traffic/outage/; Santosh Janardhan, "More details about the October 4 outage," Engineering at Meta (5 oktober 2021), https://engineering.fb.com/2021/10/05/networking-traffic/outage-details/.

15 Dave Lewis, "The DDoS Attack Against Dyn One Year Later," Forbes (23 oktober 2017), https://www.forbes.com/sites/davelewis/2017/10/23/the-ddos-attack-against-dyn-one-year-later/?sh=2f8f96991ae9.

16 Catalin Cimpanu, "Four years after the Dyn DDoS attack, critical DNS dependencies have only gone up," ZDNet (30 november 2020), https://www.zdnet.com/article/four-years-after-the-dyn-ddos-attack-critical-dns-dependencies-have-only-gone-up/; Aqsa Kashaf, Vyas Sekar, Yuvraj Agarwal, "Analyzing Third Party Service Dependencies in Modern Web Services: Have We Learned from the Mirai-Dyn Incident?," IMC '20, Virtual Event (27-29 oktober 2020), https://dl.acm.org/doi/pdf/10.1145/3419394.3423664.

17 Stephan Vegelien, "Nederlandse zeekabels verouderen: 'Digitale sleutelpositie in gevaar'," Tweakers (15 juni 2021), https://tweakers.net/reviews/9070/all/nederlandse-zeekabels-verouderen-digitale-sleutelpositie-in-gevaar.html.

Dit heeft te maken met het lastige vergunningentraject voor het aanleggen van kabels in de Noordzee, partijen kiezen ervoor om dat te omzeilen en andere routes/locaties te kiezen. Dit heeft niet echt een groot effect op de stabiliteit van het Internet, maar het is ook niet geheel zonder risico. De kortste afstand voor dataverkeer is belangrijk, met name vanuit economisch oogpunt, maar toch ook in zekere mate voor het functioneren van het internet. Zeekabels kunnen wel doelwit zijn van bijvoorbeeld spionage of sabotage activiteiten (dit wordt geadresseerd binnen de dreigingscategorie spionage dat opgenomen is in het dreigingsthema ongewenste inmenging en beïnvloeding democratische rechtsstaat.

Geopolitieke ontwikkelingen voeden het debat over digitale autonomie

De roep om digitale soevereiniteit/autonomie heeft een geopolitieke oorsprong, maar voor oplossingen wordt met name naar techniek gekeken. Daar kunnen spanningen uit naar voren komen. Door de toenemende discussie rondom digitale soevereiniteit wordt ook anders gekeken naar het internet en de (verschuivende) rol van dominante leveranciers. Voorheen lag de nadruk op kansen die internet en digitalisering bieden en daarmee was ook het propageren van het open internet dominant. Nu ontstaat steeds meer een tendens om de manier waarop het open internet functioneert als een risico te zien (want het afhankelijk zijn van partijen uit andere landen wordt bijna per definitie als bedreigend ervaren). Vanuit de robuustheid van functioneren van het internet kan dit een zorgelijke ontwikkeling zijn omdat het beeld dreigt te ontstaat dat landen zelf de technische infrastructuur kunnen ontwikkelen en beheren, terwijl dat technisch niet mogelijk/realistisch is. Wel is het belangrijk dat er gekeken wordt naar manieren om Nederland (en de EU) minder afhankelijk te maken van andere landen en in te zetten op alternatieven. [18]

De recent aangekondigde nieuwe Europese regelgeving *(EU Digital Services Act en EU Digital Markets Act)* [19] laat zien dat de EU haar digitale soevereiniteit belangrijk vindt en een leider wil worden op het gebied van digitale regulering en online contentmoderatie.

Discussies over onder andere het risico op 'achterdeurtjes' die kunnen worden ingebouwd in technologie om bijvoorbeeld spionage mogelijk te maken belemmeren het komen tot wereldwijde afspraken. Hiermee hebben geopolitieke afwegingen direct impact op de ontwikkeling van de digitale infrastructuur. Een voorbeeld is het Europese initiatief GAIA-X. Er zijn twee verschillende denkwijzen die op gespannen voet staan en het traject ook bemoeilijken. Enerzijds de denkwijze die erop gericht is om manieren te vinden om Europese waarden te waarborgen/af te dwingen, ongeacht welke partij uit welk land iets levert. Partijen worden toegelaten tot bewezen is dat ze zich schuldig maken aan onacceptabele handelingen. Anderzijds de denkwijze dat niet-Europese partijen per definitie buiten het initiatief moeten worden houden.

Belang van redundantie voor NTP

Het *Network Time Protocol* (NTP) maakt gebruik van satellietsystemen (GNSS) voor het tijdsynchronisatie mechanisme. Vanuit de soevereiniteitsdiscussie is er steeds meer aandacht voor de mogelijkheid dat de VS het gebruik van GPS kan gaan inperken of anderszins controleren. Veel organisaties gebruiken op dit moment alleen GPS voor NTP tijdsynchronisatie, maar in toenemende mate zijn er partijen die zowel GPS als GALILEO gebruiken, waardoor er redundantie ontstaat. De servers van SIDN [20] ontvangen bijvoorbeeld beide signalen en bij een verschil zal er via de interne klok een arbitrage mechanisme zijn, waardoor het geheel minder kwetsbaar wordt voor storing. De investering om dit soort redundantie in te regelen zal voor veel partijen niet heel groot zijn, maar de drempel om dit te doen is – net als bij andere maatregelen – vermoedelijk toch vrij groot.

Cryptografie wordt steeds belangrijker

Cryptografie is in toenemende mate belangrijk voor het functioneren van het internet (specifiek gaat het om cryptografische algoritmen die onderdeel vormen van veel internet protocollen). End-to-end encryptie zorgt ervoor dat de privacy en veiligheid van online gegevens voor gebruikers van internetdiensten worden beschermd. Tegelijkertijd wordt zicht krijgen op criminele activiteit op het internet steeds moeilijker, wat een probleem is vanuit het oogpunt van opsporing en handhaving. Dit spanningsveld zorgt voor een stevig debat over de rol van encryptie. [21]

[18] Cyber Security Raad, "'Digitale autonomie Nederland staat onder druk'," Cyber Security Raad (14 mei 2021), https://www.cybersecurityraad.nl/actueel/nieuws/2021/05/14/%E2%80%98digitale-autonomie-nederland-staat-onder-druk%E2%80%99.

[19] Rijksoverheid, "EU-ministers akkoord met regelgeving voor digitale diensten en markten," Rijksoverheid (25 november 2021), https://www.rijksoverheid.nl/actueel/nieuws/2021/11/24/eu-ministers-akkoord-met-regelgeving-digitale-diensten-en—markten.

[20] Marco Davids, "Goede dingen hebben tijd nodig: Een update over onze publieke NTP-dienst TimeNL," SIDN Labs (19 april 2021), https://www.sidnlabs.nl/nieuws-en-blogs/goede-dingen-hebben-tijd-nodig. https://www.sidnlabs.nl/nieuws-en-blogs/goede-dingen-hebben-tijd-nodig

[21] Maria Koomen, "The Encryption Debate in the European Union: 2021 Update," Carnegie Endowment for International Peace International Encryption Brief (31 maart 2021), https://carnegieendowment.org/2021/03/31/encryption-debate-in-european-union-2021-update-pub-84217.

Ook in dit kader speelt de discussie over autonomie/soevereiniteit een rol. Er zijn ontwikkelingen waarbij cryptoaanbieders uit bepaalde landen worden verplicht om een *master-key* in te bouwen voor hun nationale overheden. Hiermee kan de betreffende overheid *encrypted* data ontsleutelen. Er zijn vermoedens (maar dit is niet bewezen) dat dit voor Chinese aanbieders al geldt.
In de VS [22] en het VK [23] is in de afgelopen jaren wetgeving voorgesteld waarbij aanbieders ook zouden worden gedwongen om mogelijkheden in te bouwen waarbij de overheid in specifieke gevallen toegang moet kunnen krijgen tot de data. Dit type regelgeving stuit op veel weerstand omdat dit de manier waarop encryptie bijdraagt aan het veilig functioneren van het internet verzwakt. De ingebouwde '*backdoor*' die door de wetgeving door overheidspartijen gebruikt zou kunnen worden, is ook een kwetsbaarheid voor kwaadwillenden en maakt de encryptie minder sterk. [24]

Op langere termijn kan *quantum computing* ervoor zorgen dat de cryptografie die wordt gebruikt in veel internetprotocollen niet meer voldoet. Om die reden is er toenemende aandacht voor post-quantum cryptografie. Dit betekent echter ook dat de manier waarop veel internetprotocollen nu werken daar ook op aangepast zal moeten worden en dat zal nog veel voeten in de aarde gaan hebben. [25]

Stagnerende uptake van maatregelen

In algemene zin is het een zorg dat maatregelen om het functioneren van het internet te behouden niet door alle gebruikers snel worden overgenomen. Het toepassen van maatregelen vraagt vaak om ingrijpende aanpassingen van configuraties en dat wordt door gebruikers ervaren als een belemmering. De urgentie van de problemen die op den duur kunnen ontstaan wordt onvoldoende gevoeld, of weegt niet voldoende op tegen de moeite die het kost om de maatregelen op te pakken.

Voor het blijven functioneren van internet is bijvoorbeeld de stagnerende uptake van IPv6 een zorg. IPv6 is de opvolger van IPv4 en moet het dreigende tekort aan IP-adressen oplossen. De IPv4 ruimte is op, dus het achterblijven van IPv6 uptake zou op den duur problemen kunnen opleveren voor het goed functioneren van het internet.

Ook als het gaat om belangrijke veiligheidsmaatregelen zoals RPKI, DNSSEC en anti-spoofing (BCP38) verloopt de uptake langzaam of blijft achter. Voor RPKI en DNSSEC geldt wel dat er in de afgelopen tijd grote stappen zijn gezet, maar toch lijkt de voortgang van met name de uptake van DNSSEC te stagneren, waardoor bepaalde kwetsbaarheden toch blijven bestaan.

De komst van 5G in combinatie met '*network slicing*'

De komst van 5G en de toenemende behoefte aan *edge computing* (noodzaak van een kleine *latency* voor real time services), in combinatie met de mogelijkheid van sectorale specificering van diensten (via *network slicing*, een vorm van virtualisatie op het niveau van een netwerk [26]) kan er in de toekomst toe leiden dat de diensten aan specifieke veiligheid georiënteerde afnemers (bijvoorbeeld voor noodcommunicatie (C2000) of andere vitale processen) niet meer op een apart netwerk worden aangeboden, maar als 'network slice' op de generieke infrastructuur (5G netwerk). Voordeel hiervan is de kwaliteit en professionaliteit van de infrastructuur, maar dit kan potentieel ook weer kwetsbaarheden met zich meebrengen vanuit (nationaal) veiligheidsoogpunt. [27]

Relatie ontwikkelingen van digitale infrastructuur met klimaatverandering en energietransitie

Digitale systemen zijn grootverbruikers van energie en dat kan zorgen voor weerstand en spanningsvelden tussen verschillende belangen. Manifestaties van deze spanningen zijn bijvoorbeeld de discussies over de mogelijke komst van grote datacenters in Nederland waarbij verschillende belangen op zeer gespannen voet staan. [28]

---

22 Kenneth Olmstead, Ryan Polk, "Latest U.S. 'Anti-Encryption' Bill Threatens Security of Millions," Internet Society (7 juli 2020), https://www.internetsociety.org/blog/2020/07/latest-u-s-anti-encryption-bill-threatens-security-of-millions/.

23 Callum Voge, "UK Online Safety Bill Set to Weaken Encryption and Put UK Internet Users At Risk," Internet Society (19 januari 2022), https://www.internetsociety.org/blog/2022/01/uk-online-safety-bill-set-to-weaken-encryption-and-put-uk-internet-users-at-risk/.

24 Global Encryption Coalition, "Internet Society Open Letter Against Lawful Access to Encrypted Data Act," Global Encryption Coalition (7 juli 2020), https://www.globalencryption.org/2020/07/internet-society-open-letter-against-lawful-access-to-encrypted-data-act/.

25 Moritz Müller, Jins de Jong, Maran van Heesch, Benno Overeinder en Roland van Rijswijk-Deij, "Retrofitting post-quantum cryptography in Internet protocols: A case study of DNSSEC," ACM SIGCOMM Computer Communication Review 50, no.4 (oktober 2020): 49-57, https://www.sidnlabs.nl/downloads/7qGFWoDiOkovovWyDK9qaK/de709198ac34477797b381f146639e27/Retrofitting_Post-Quantum_Cryptography_in_Internet_Protocols.pdf.

26 Alex Mathew, "Network Slicing in 5G and the Security Concerns," Proceedings of the Fourth International Conference on Computing Methodologies and Communication (ICCMC 2020), 10.1109/ICCMC48092.2020.ICCMC-00014.

27 Ruxandra F. Olimid, Gianfranco Nencioni, "5G Network Slicing: A Security Overview," IEEE Access 8 (mei 2020), https://ieeexplore.ieee.org/stamp/stamp.jsp?arnumber=9099823.

28 Paolo Laconi, "Zo kwam Europa's grootste datacentrum in een polder bij Zeewolde," De Stentor (23 januari 2022), https://www.destentor.nl/zeewolde/zo-kwam-europas-grootste-datacentrum-in-een-polder-bij-zeewolde~a82dbd49/.

3.2 Overzicht van mogelijke actoren en factoren

Binnen deze categorie gaat het over gebeurtenissen die ervoor zorgen dat het functioneren van het internet en internetdiensten wordt aangetast. Hoewel de toegang van gebruikers tot internet en internetdiensten op heel veel manieren kan worden belemmerd, bijvoorbeeld door een verstoring van de elektriciteitsvoorziening, gaat het in deze categorie om verstoringen van het functioneren die veroorzaakt worden door elementen in de internet-infrastructuur zelf. Om voor de analyse een keuze te maken tussen de veelheid aan mogelijke dreigingsscenario's is een overzicht gemaakt van de belangrijkste factoren (bouwstenen) die karakteriserend zijn voor verschillende typen verstoringen.

De **oorzaak** kan een moedwillige of niet-moedwillige aard hebben (waarbij nog onderscheid gemaakt kan worden tussen technisch of menselijk falen). Voor moedwillige gebeurtenissen is het van belang om onderscheid te maken tussen verschillende typen **actoren** en het **motief** dat zij hebben om een aanval uit te voeren. De aantasting kan betrekking hebben op verschillende **elementen** die een rol spelen bij het functioneren van het Internet [29], hoewel er ook sprake kan zijn van een combinatie van elementen die aangetast worden. De manier waarop de aantasting ontstaat heeft voorts te maken met de (combinatie van) **middelen** die gebruikt worden of optreden (misconfiguratie of fysieke aantasting kan zowel een moedwillig als niet-moedwillige aanleiding hebben). [30] Ook hiervoor geldt dat in de praktijk vaak een combinatie van verschillende middelen een rol speelt in een gebeurtenis.

Als het gaat om de impact van een gebeurtenis wordt onderscheid gemaakt in de **aard van de aantasting** (beschikbaarheid, integriteit of vertrouwelijkheid), waarbij het in deze dreigingscategorie veelal zal gaan om beschikbaarheid, eventueel in combinatie met andere vormen van aantasting. Verder kan de aantasting verschillende categorieën van organisaties treffen, waarbij het ook relevant kan zijn om onderscheid te maken tussen direct **getroffen partijen** en partijen die in tweede orde getroffen worden (bijvoorbeeld in geval van een supply chain aanval). De omvang en ernst van een aantasting van het functioneren van het internet is verder lastig in concrete factoren uit te drukken omdat dit heel er afhangt van het type situatie. De **doordringingsgraad** (mate van verspreiding binnen en tussen categorieën van getroffen partijen) en **duur** van de aantasting zijn twee belangrijke factoren die van invloed zijn op de ernst van de impact.

[29] Gebaseerd op van Ruijven, Duijnhoven, Overeinder, Akkerhuis, "ANV Verkenning t.b.v. de risicocategorie Aantasten functioneren Internet".

[30] In de praktijk wordt bij aanvallen ook vaak een combinatie van technieken gebruikt.

Tabel 4 Factoren en actoren dreigingscategorie aantasting functioneren internet

Oorzaak	Actor	Motief	Element	Middelen	Aard van de aantasting	Getroffenen (direct)	Getroffenen (keteneffecten)	Doordringings-graad	Duur
Technisch falen	Criminelen [31]	Economisch gewin	DNS (rootservers, name servers, DNS operators)	Distributed Denial of Service (DDoS)	Aantasting van beschikbaarheid	Vitale aanbieders	Vitale aanbieders	Klein deel van de betreffende categorieën is getroffen (<10%)	Tot 1 dag
Menselijk falen	Statelijke actoren	Ideologische doelstelling	BGP (routing tables)	Misconfiguratie	Aantasting van integriteit	Rijksoverheid	Rijksoverheid	Aanzienlijk deel van de betreffende categorieën is getroffen (10-50%)	2 tot 6 dagen
Moedwillig	Terroristen	(Geo-) Politieke doelstelling	NTP	Fysieke aantasting (explosie, kabel stuk, etc.)	Aantasting van vertrouwelijkheid	Digitale dienstverleners	Digitale dienstverleners	Merendeel van de betreffende categorieën is getroffen is getroffen (>50%)	1 tot 4 weken
	Cyber-vandalen en scriptkiddies	Ego, profilering of wraak	Internet infrastructuur (e.g. kabels, IX-en, datacenters)	Malware infectie (inclusief ransomware)		Topsectoren	Topsectoren		1 tot 6 maanden
	Hacktivisten		Vertrouwens-diensten (e.g. certificaten, public key infrastructure)	Misbruik van kwetsbaarheden		Kennisinstellingen	Kennisinstellingen		Half jaar of langer
	Interne actoren		...	Social engineering (incl. phishing)		Overige organisaties (incl. gemeenten, veiligheidsregio's, MKB)	Overige organisaties (incl. gemeenten, veiligheidsregio's, MKB)		Onherstelbaar
	Cyberonderzoekers			...		Burgers	Burgers		
	Private organisaties								

[31] Dit omvat zowel autonome criminele samenwerkingsverbanden, dienstverleners van zgn. 'cybercrime-as-a-service' en individuele cybercriminelen.

3.3 Scenario's

Zoals ook uit het overzicht van factoren naar voren komt, zijn er heel veel mogelijke gebeurtenissen die het functioneren van het internet kunnen aantasten. In de selectie van dreigingsscenario's heeft een aantal aspecten een belangrijke rol gespeeld. Zo is er gekozen voor zowel een moedwillig als een niet-moedwillig (menselijk falen) scenario. Ook het mondiale karakter van het internet is belangrijk om mee te nemen. Om die reden richt één scenario richt zich op een verstoring vanuit een grote mondiale aanbieder met wereldwijde effecten en één scenario richt zich op een verstoring op Nederlands grondgebied, waarbij de gevolgen zich dan ook voornamelijk binnen een groep Nederlandse gebruikers concentreren. Ook de variëteit in elementen en middelen die een rol spelen in de gebeurtenissen is van invloed geweest op de selectie. Beide scenario's zijn omvangrijk maar kennen ook grote onzekerheid in de mogelijke effecten. De duur van de verstoringen is in beide scenario's beperkt tot één of enkele dagen, al wordt dat door experts als relatief lang ingeschat ten opzichte van gebeurtenissen in de praktijk.

Naast de twee reguliere scenario's is ervoor gekozen om een wild-card-scenario op te nemen dat als een potentieel *game-changing* gebeurtenis kan worden gezien voor de huidige internet governance.

Reguliere Scenario's
Misconfiguratie grote internetdienstverlener
Aanval Cloud Service Provider
Wild-card-scenario
Sabotage DNSSEC

Tabel 5 Factoren scenario misconfiguratie grote internetdienstverlener

Oorzaak	Actor	Element	Middelen	Aard van de aantasting
Menselijk falen	Interne actoren	DNS (rootservers, name servers, DNS operators)	Misconfiguratie	Aantasting van beschikbaarheid
		BGP (routing tables)		

Tabel 5 Factoren scenario misconfiguratie grote internetdienstverlener (vervolg)

Getroffenen (direct)	Getroffenen (keteneffecten)	Doordringingsgraad	Duur
Digitale dienstverleners	Vitale aanbieders	Aanzienlijk deel van de betreffende categorieën is getroffen (10-50%)	Tot 1 dag
	Digitale dienstverleners		
	Topsectoren		
	Kennis instellingen		
	Overige organisaties (incl. gemeenten, veiligheidsregio's, MKB)		
	Burgers		

3.3.1 Scenario misconfiguratie grote internetdienstverlener

Dit scenario is geïnspireerd op de Facebook storing in oktober 2021, toen alle diensten van Facebook (nu Meta) gedurende ongeveer 8 uur wereldwijd niet beschikbaar waren. Dit werd veroorzaakt door een misconfiguratie die ernstige gevolgen had voor de interne *backbone* van hun systemen en netwerken. Wat met name uit dit incident naar voren kwam is dat de complexiteit van het interne netwerk van Facebook ervoor zorgde dat het herstel werd belemmerd.

Ook in de samenleving liet dit incident duidelijk zien hoeveel diensten afhankelijk zijn van het netwerk van deze dienstverlener. Toch was de impact, zeker vanuit het oogpunt van nationale veiligheid, relatief beperkt. De vraag die wel rees is wat er zou kunnen gebeuren als een vergelijkbare storing optreedt bij één van de grootste wereldwijde internetdienstverleners, de zogenoemde 'hyperscalers' of 'techgiganten'. Deze dienstverleners, zoals Amazon Web Services, Microsoft en Google, leveren heel veel uiteenlopende diensten en componenten die verborgen zitten in allerlei systemen en netwerken wereldwijd. Ook leunen deze organisaties sterk op hun eigen technologie en interne *backbone* voor het leveren van diensten. De kwaliteit en expertise van deze organisaties is enorm en over het algemeen willen zij zo min mogelijk afhankelijk zijn van andere partijen, maar dit kan wellicht ook betekenen dat er steeds meer onbekende afhankelijkheden in hun systemen zitten, waardoor – net als bij Facebook – de storing zich verder kan verspreiden én herstel bemoeilijkt zou kunnen worden.

Bovenstaande was, in afstemming met experts, dan ook de aanleiding voor de keuze van het scenario dat voor deze analyse is uitgewerkt: een misconfiguratie bij een grote internetdienstverlener. In het scenario wordt geschetst wat voor type systemen allemaal geraakt kunnen worden (slimme apparaten, *Internet of Things* (IoT) systemen, toegangssystemen, gebouwbeheersystemen, kantoor-automatiseringsdiensten, clouddiensten, etc.). Maar wát er precies allemaal uitvalt is bewust in het midden gelaten. Dit komt namelijk overeen met de onzekerheid die er heerst onder experts over de gevolgen van een dergelijke storing.

Bouwstenen

In Tabel 5 is het scenario weergegeven aan de hand van de factoren en actoren.

Verhaallijn

Bij één van de grote, mondiale internetdienstverleners [32] wordt tijdens routine onderhoud aan de interne systemen een configuratiefout gemaakt. Door de hoge mate van automatisering en onderliggende afhankelijkheden in de systemen van het bedrijf wordt deze fout onmiddellijk aan andere systemen doorgegeven, wat tot een opeenstapeling van problemen leidt. De routers van de interne *backbone* van het bedrijf vallen uit en dat zorgt ervoor dat DNS-servers geen connecties meer hebben naar de centrale systemen met actuele routing informatie van het bedrijf. Omdat dergelijke netwerkisolatie kan leiden tot onwenselijk gedrag (bijvoorbeeld dat enkele servers na verloop van tijd verouderde routing data publiceren, waardoor netwerk-verkeer niet over de juiste paden verloopt), zijn de servers geprogrammeerd om de door hen geadverteerde BGP-routes aan naburige netwerken in te trekken. Omdat naburige netwerken vanaf dat moment geen actuele routing informatie naar het bedrijf meer hebben, raken de systemen van dit bedrijf effectief ontkoppeld van het internet.

Het gevolg hiervan is dat allerlei applicaties, diensten en systemen die op een of andere manier gebruik maken van de infrastructuur van de betreffende aanbieder verstoord raken. Omdat deze aanbieder heel veel zogenaamde componenten levert aan gebruikers in de hele wereld zijn de effecten heel wijdverspreid en onverwacht. Veel gebruikers zijn zich niet bewust dat ze zo afhankelijk zijn van de beschikbaarheid van deze aanbieder en er ontstaat veel onrust en chaos.

Heel veel organisaties en consumenten worden getroffen. De betreffende aanbieder levert ook veel componenten die gebruikt worden in allerlei slimme apparaten met een internetverbinding, zoals koelkasten, thermostaten, smartwatches en deurbellen. Deze verliezen hun verbinding en gaan in '*fallback modus*', waardoor ze niet meer op afstand bestuurd en uitgelezen kunnen worden. Ook toegangs-systemen en andere gebouwbeheersystemen van verschil-lende grote en kleine organisaties vallen uit, waardoor men de panden van deze gebouwen niet meer kan betreden of verlaten, of waardoor andere problemen ontstaan.

Ook gebruikers van de clouddiensten van deze aanbieder ondervinden veel hinder. Bedrijven en overheden kunnen geen gebruik meer maken van kantoorautomatiserings-diensten de het bedrijf aanbiedt, automatische data-uitwisseling tussen systemen komt stil te liggen, online portalen van verschillende overheden zijn niet meer bereikbaar. De verstoring zorgt bij bedrijven voor veel verwarring en leidt ertoe dat veel bedrijfsprocessen stil

[32] Zoals Microsoft, Google, of Amazon Web Services.

komen te liggen, niet alleen vanwege de daadwerkelijke verstoring maar ook deels uit voorzorg omdat men onzeker is over wat er allemaal geraakt is en mis zou kunnen gaan. Er ontstaan lange files op de snelwegen en er is grote drukte in het openbaar vervoer omdat thuiswerken - wat sinds de coronacrisis steeds meer een norm geworden is - ineens niet meer mogelijk is.

Na zo'n 10 uur krijgt de aanbieder het voor elkaar de fout te achterhalen en te herstellen. Het duurt vervolgens nog een aantal uur om alle systemen langzaam weer op te starten en de verschillende diensten weer online te brengen. Omdat er bij het opstarten een enorme hoeveelheid dataverkeer zal ontstaan moet dit gefaseerd gedaan worden, want anders zal overbelasting ervoor zorgen dat systemen direct weer uit kunnen vallen.
De meeste functionaliteiten zijn voor het bedrijf en haar klanten na 12 uur weer hersteld, al duurt het nog dagen om de systemen geheel te herstellen. Sommige van de klanten ondervinden nog dagen haperingen en beperkte bereikbaarheid in het gebruik van diensten en producten.

Beoordeling van de impact en waarschijnlijkheid

Het is duidelijk dat de diensten van dit type internetdienstverlener zéér wijdverspreid zijn, maar door de complexiteit van het landschap is het vrijwel onmogelijk om te voorspellen wat er precies gaat gebeuren als er een grootschalige storing optreedt. Experts benadrukken dat het zelfs voor individuele organisaties moeilijk is om de afhankelijkheid van dergelijke componenten voor de eigen operationele processen goed in beeld te hebben, laat staan dat er een duidelijk beeld is van de gevolgen op het niveau van de samenleving. Het is zeker dat een dergelijke storing op heel veel plekken en voor heel veel verschillende typen organisaties merkbaar zal zijn. Maar in hoeverre dit tot ernstige problemen zal leiden is veel moeilijker in te schatten. Verder geven experts aan dat de verwachting is dat de afhankelijkheid van dit type aanbieder in de toekomst zal blijven toenemen, waardoor de impact kan toenemen.

Een belangrijke vraag voor het bepalen van de impact is in welke mate **vitale processen** geraakt kunnen worden. Ook dit is heel lastig in te schatten. Hoewel continuïteit een belangrijk aandachtspunt is voor aanbieders van vitale processen, is het zeer aannemelijk dat ook zij op enige manier gebruik maken van diensten van een dergelijke grote aanbieder. Zelfs wanneer dit niet in de primaire operationele processen zit (wat ook niet uitgesloten kan worden), kunnen zij er op allerlei andere manieren wel hinder van ondervinden (bijvoorbeeld in de kantoorautomatisering of gebouwbeheersystemen) en dat kan uiteindelijk ook gevolgen hebben voor de continuïteit van vitale processen. Het is dus zeker niet uit te sluiten dat er flinke impact ontstaat. Experts geven aan dat er enkele vitale processen zijn waarbij het minder voor de hand ligt dat er impact ontstaat vanuit dit type gebeurtenis:
Plaats- en tijdsbepaling middels GNSS zal hoogstwaarschijnlijk niet geraakt worden en ook bij **vlucht- en vliegtuigafhandeling** wordt veelal van onafhankelijke systemen gebruik gemaakt, waardoor dit vermoedelijk gewoon door kan blijven gaan. De **inzet van politie en defensie** zal vermoedelijk niet verstoord raken. Ook **C2000** zal niet verstoord raken omdat dit op een apart netwerk draait. De **olievoorziening** zal vermoedelijk niet geraakt worden al kunnen er wel logistieke problemen optreden. Ook de **opslag, productie en verwerking van nucleair materiaal** zal hierdoor naar verwachting niet geraakt worden.

Voor de overige vitale processen is de te verwachten impact onzeker. Dit betekent ook dat de impactbeoordeling zoals weergegeven in onderstaand overzicht ook enige mate van onzekerheid kent.

Tabel 6 Scorekaart scenario misconfiguratie grote internetdienstverlener

Thema	Cyberdreigingen		
Dreigingscategorie	Aantasting functioneren internet		
Scenario	Misconfiguratie grote internetdienstverlener		
Scenariotoelichting	Door een interne misconfiguratie ontstaat er een BGP storing waardoor de diensten van een grote (internationale) internetdienstverlener onbereikbaar zijn. Het duurt ca. 10 uur om de storing te verhelpen waarna die diensten geleidelijk weer bereikbaar worden. Heel veel organisaties wereldwijd hebben hier last van, ook vanwege de vele componenten van deze dienstverlener die in systemen zitten.		
Waarschijnlijkheidsbeoordeling (binnen 5 jaar)			**Toelichting**
Waarschijnlijkheid:		D	Het is absoluut waarschijnlijk dat een dergelijke gebeurtenis binnen 5 jaar bij een grote dienstverlener (hyperscaler) gaat optreden. Recente verstoringen door misconfiguraties bij Facebook en Slack laten dit zien. Een duur van 10 uur is wel relatief lang, en er wordt ook geleerd van recente incidenten, maar tegelijkertijd zijn er steeds meer (verborgen) afhankelijkheden in systemen waardoor herstel bemoeilijkt kan worden.
Beoordeling gevolgen (impact)			
Veiligheidsbelang	**Criterium**	**Score**	**Toelichting**
Territoriaal	1.1 Grondgebied	0	Niet van toepassing
	1.2 Internationale positie	0	Niet van toepassing: geen Nederlands bedrijf, grote multinational uit ander land, Nederland wordt hier niet op aangekeken. Het kan wel zo zijn dat internationale organisaties in Nederland problemen ondervinden en dat dit effect heeft op imago van Nederland, maar de verwachting is niet dat dit zal leiden tot een score op de indicatoren binnen dit criterium.
	1.3 Digitale ruimte	B	De misconfiguratie zelf leidt niet direct tot ongewenste toegang tot systemen, maar het is denkbaar dat in reactie hierop bedrijven creatieve *workarounds* gaan gebruiken om toch te kunnen werken, waardoor er kwetsbaarheden ontstaan die misbruikt kunnen worden (dat is dan een *window of opportunity* voor kwaadwillenden). De verwachting is dat vitale aanbieders hier bedachtzamer mee omgaan dan andere (commerciële) organisaties of bv. Rijksoverheid en gemeenten. Er is geen sprake van een verzwaring door motief of omvang.
	1.4 Bondgenootschappelijk grondgebied	0	Niet van toepassing

Veiligheidsbelang	Criterium	Score	Toelichting
Fysiek	2.1 Doden	A	Het is denkbaar dat er enkele slachtoffers vallen door gevolgschade van verstoringen bij klanten van de dienstverlener. Dit type internetdiensteverleners maken een groot deel uit van onze infrastructuur en supply chains en daar zitten risico's. Lastig in te schatten wat daar precies wel en niet in zit en hoe dat precies tot uiting zou komen.
	2.2 Ernstig gewonden en chronisch zieken	A	Het is denkbaar dat er enkele slachtoffers vallen door gevolgschade van verstoringen bij klanten van de dienstverlener. Dit type internetdiensteverleners maken een groot deel uit van onze infrastructuur en supply chains en daar zitten risico's. Lastig in te schatten wat daar precies wel en niet in zit en hoe dat precies tot uiting zou komen.
	2.3 Gebrek primaire levensbehoeften	0	Niet van toepassing: Hoewel de impact langer kan duren dan 10u, omdat (cascade) effecten nog na ijlen, is niet de verwachting dat er een gebrek zal ontstaan aan primaire levensbehoeften.
Economisch	3.1 Kosten	B	Er zal flink wat financiële schade optreden bij getroffen bedrijven, maar vanwege de relatief korte duur zal dat met name sectoren treffen waarbij de omzet niet in de dagen erna ingehaald kan worden. Waar de schade precies optreedt is moeilijk in te schatten, maar uitgaande van een verlies van 2%-5% van de Nederlandse economie per dag is de verwachting dat het denkbaar is dat het meer dan 50 miljoen betreft (vergelijking met bijvoorbeeld de aswolk van de IJslandse vulkaan waarbij er alleen al bij KLM 10 miljoen schade was per dag).
	3.2 Aantasting vitaliteit	0	Niet van toepassing
Ecologisch	4.1 Aantasting natuur en milieu	0	Niet van toepassing
Sociaal-politiek	5.1 Verstoring dagelijks leven	C	3 à 4 indicatoren (duur 1 à 2 dagen). Het zal bij drie indicatoren al snel om >100.000 getroffenen gaan. Het is zelfs niet ondenkbaar dat het >1 miljoen mensen zal treffen (dus: gemiddeld) **Onderwijs**: steeds afhankelijker van digitale systemen (onderwijs van hele instellingen wordt stilgelegd) **Werk**: afhankelijk van welke diensten verstoord zijn kan dat omvangrijk zijn al is er bij veel organisaties nog wel werk dat wél gedaan kan worden. **Maatschappelijke voorzieningen**: denkbaar dat bijvoorbeeld fysio- of huisartsen afspraken niet door kunnen gaan. Beperktere omvang, <10.000 getroffenen **Virtuele/sociale bereikbaarheid** kan aangetast worden (afhankelijk van diensten die verstoord raken en er zijn alternatieven).

Veiligheidsbelang	Criterium	Score	Toelichting
	5.2 Aantasting democratische rechtsstaat	0	Niet van toepassing
	5.3 Sociaal-maatschappelijke impact	A	Er zal sprake zijn van onrust, onduidelijkheid wat er aan de hand is, maar omdat e.e.a. vrij snel hersteld. Eerste paar uur zal er nog wel begrip zijn, als het wat langer duurt zal er wel sprake zijn van meer verontwaardiging richting techbedrijven of andere partijen die geraakt zijn, maar het is niet de verwachting dat mensen de straat op gaan hoewel dit ook niet helemaal ondenkbaar is als er sprake is van een stapeleffect omdat er al meer aan de hand is in de samenleving en deze uitval komt daar bovenop. *Bovengrens zou eventueel B zijn.*
Internationale rechtsorde en stabiliteit	6.1 Staatssoevereiniteit, vreedzame co-existentie en vreedzame geschillenbeslechting	0	Niet van toepassing
	6.2 Mensenrechten	0	Niet van toepassing
	6.3 Internationaal financieel-economisch bestel	0	Niet van toepassing
	6.4 Multilaterale instituties	0	Niet van toepassing
	6.5 Instabiliteit rondom Koninkrijk/EU	0	Niet van toepassing

3.3.2 Scenario aanval Cloud Service Provider

Vanwege de steeds grotere rol van clouddiensten in het internetlandschap is ervoor gekozen om een scenario uit te werken dat betrekking heeft op een clouddiensten leverancier (Cloud Service Provider, CSP). Recent heeft TNO op verzoek van de NCTV een dreigingsscenario gericht op clouddiensten uitgewerkt voor het Cyber Security Beeld Nederland 2021 [33] en dit scenario vormt een goed startpunt voor voor de risicoanalyse in de RbRa. Vanwege de iets andere scope is ervoor gekozen om een verkorte variant van het scenario uit het CSBN te gebruiken in deze analyse. Het betreft een moedwillige aanval op een in Nederland gelegen datacenter van een grote CSP, waarbij de aanvallers een interne DDoS aanval uitvoeren met als gevolg een crash van virtuele machines die op dat moment actief waren. De crash raakt een deel van de Nederlandse klanten van de CSP en kan – afhankelijk van de specifieke configuratie van de clouddiensten die klanten afnemen – leiden tot het tijdelijk niet beschikbaar zijn van clouddiensten of zelfs het verlies van data.

In het scenario komt naar voren dat er aanwijzingen zijn dat de aanvallers gelinkt zijn aan een statelijke actor en het vermoeden bestaat dat de crash is veroorzaakt om sporen van data-exfiltratie uit te wissen. In de praktijk blijkt dat aanvallers vaak verschillende typen aanvallen combineren en dat criminele groeperingen zich ook vaak laten inhuren door statelijke actoren. Veel incidenten zijn dan ook niet heel eenduidig te classificeren en komen er verschillende fenomenen samen (in dit geval sabotage en spionage).

Net als bij het scenario misconfiguratie grote internet-ienstverlener is de impact van deze gebeurtenissen moeilijk in te schatten omdat dit sterk afhangt van de manier waarop afnemers clouddiensten inrichten en gebruiken, en of er maatregelen zijn getroffen die het verlies van gegevens kan voorkomen (zoals goede back-up maatregelen).

Bouwstenen

In Tabel 7 is het scenario weergegeven aan de hand van de factoren en actoren.

Verhaallijn

Een grote groep Nederlandse klanten van de CSP Cirrocumulus Networks heeft plotseling geen toegang tot hun cloudomgeving. Berichten in de media wijzen direct op een grootschalige storing in de infrastructuur van Cirrocumulus Networks, waarbij de mogelijkheid dat het om een aanval gaat niet wordt uitgesloten. Opvallend is dat dit gebeurt in een periode waarin al eerder berichten naar buiten zijn gekomen over verdachte activiteiten in de cloudomgeving van meerdere klanten van Cirrocumulus Networks. Een woordvoerder van Cirrocumulus Networks geeft aan dat er inderdaad sprake is van een verstoorde dienstverlening door problemen in een van haar datacentra en dat zij bezig zijn met het zoeken naar de oorzaak en oplossing. Ondertussen groeit de onrust onder klanten van Cirrocumulus Networks, gevoed door berichten in de media. Zijn hun systemen en data nog wel betrouwbaar en veilig? Wat is hier aan de hand?

Tabel 7 factoren scenario Aanval Cloud Service Provider

Oorzaak	Actor	Motief	Element	Middelen
Moedwillig	Criminelen [34]	Economisch gewin	Internet infrastructuur (e.g. kabels, IX-en, data-centers)	Distributed Denial of Service (DDoS)
	Statelijke actoren	(Geo-) Politieke doelstelling		Malware infectie (inclusief ransomware)
				Misbruik van kwetsbaarheden

33 NCTV, *Cybersecuritybeeld Nederland (CSBN)* 2021.

34 Dit omvat zowel autonome criminele samenwerkingsverbanden, dienstverleners van zgn. 'cybercrime-as-a-service' en individuele cybercriminelen.

Tabel 7 factoren scenario Aanval Cloud Service Provider (vervolg)

Aard van de aantasting	Getroffenen (direct)	Getroffenen (keteneffecten)	Doordringingsgraad	Duur
Aantasting van beschikbaarheid	Digitale dienst-verleners	Vitale aanbieders	Klein deel van de betreffende categorieën is getroffen (<10%)	2 tot 6 dagen
Aantasting van vertrouwelijkheid		Rijksoverheid		
		Digitale dienstverleners		
		Topsectoren		
		Kennis instellingen		
		Overige organisaties		
		(incl. gemeenten, veiligheidsregio's, MKB)		

Na enkele uren komt Cirrocumulus naar buiten met de mededeling dat er sprake is van een geavanceerde aanval gericht tegen een datacentrum van het bedrijf in Nederland, waardoor een deel van de Nederlandse klanten geraakt is. De situatie is inmiddels onder controle en Cirrocumulus Networks doet er alles aan om de dienstverlening zo snel mogelijk weer te herstellen. Dit kan enkele uren tot enkele weken in beslag nemen, afhankelijk van de specifieke situatie van de getroffen gebruikers.

In de dagen die volgen komt langzaam meer informatie over het incident naar buiten. Het lijkt erop dat aanvallers in staat zijn geweest om van binnenuit, via een botnet van virtuele machines, een enorme hoeveelheid verkeer te genereren. Deze interne DDoS aanval heeft de virtual machine manager (VMM) overspoeld en deze is daardoor uitgevallen. De VMM is software die de virtualisatie van de hardware (servers in een datacentrum) reguleert en de beschikbare resources zoals geheugen en CPU over de aangesloten gebruikers (virtuele machines van klanten) verdeelt. Doordat de VMM gecrasht is, zijn alle virtuele machines die verbonden waren met de VMM en die op dat moment actief waren, verloren gegaan.

Voor het herstel van de dienstverlening is de VMM gereset. Cirrocumulus Networks stemt met alle getroffen klanten af of de virtuele machines van die klant ook gereset kunnen worden of dat er eerst nadere analyse nodig is om te bepalen of gegevens, waar ten tijde van de crash aan gewerkt werd, hersteld moeten en kunnen worden. Dit hangt af van de configuratie van de cloudomgeving van een gebruiker en het type werkzaamheden die de klant op de getroffen virtuele machines uitvoert. Voor klanten waarvan (een deel van) de virtuele machines gereset worden, geldt dat zij enkele minuten of maximaal een paar uur nadat de VMM gereset wordt weer de beschikking hebben over hun cloudomgeving. Bij gebruikers waar nader onderzoek nodig is kan dit dagen of zelfs enkele weken duren.

In de berichtgeving over het incident wordt ook veel aandacht besteed aan hoe deze aanval heeft kunnen plaatsvinden. Om de virtuele machines als een botnet te laten functioneren hebben de aanvallers malware in de virtuele machines geplaatst. Dat betekent dat zij toegang moeten hebben gehad tot deze virtuele machines.
Dit gegeven leidt tot speculaties over een verband met een recent incident bij gebruikers van Cirrocumulus Networks, waarbij aanvallers in staat waren om een kwetsbaarheid te exploiteren tijdens een herstelactie na een storing.
Die aanvallers hebben zich toen toegang verschaft tot de cloudomgeving van verschillende gebruikers, vermoedelijk om data te exfiltreren. Het lijkt er nu op dat dezelfde daders toen ook zijn begonnen met het voorbereiden van deze interne DDoS aanval. Volgens experts is het goed mogelijk dat de aanvallers, nu hun activiteiten ontdekt zijn, deze DDoS aanval hebben geactiveerd om het onderzoek te bemoeilijken en zoveel mogelijk schade en hinder te veroorzaken.

Beoordeling van de impact en waarschijnlijkheid

Het gebruik van clouddienstverlening neemt al jaren flink toe en het is dan ook te verwachten dat een verstoring zoals beschreven in dit scenario een grote impact kan hebben. Toch is het voor experts lastig om de exacte impact in te schatten omdat de getroffen klanten van een Cloud Service Provider niet allemaal op dezelfde manier last zullen hebben van een dergelijk incident. De manier waarop het bedrijfsprocessen raakt heeft te maken met de manier waarop elke individuele gebruiker haar cloudomgeving heeft ingericht en welke maatregelen er getroffen zijn om in geval van verstoring snel te kunnen herstellen of effecten te beperken.

Volgens experts is het in het huidige landschap niet ondenkbaar dat bij een dergelijke aanval op één datacentrum van een CSP meerdere vitale aanbieders geraakt zullen worden. Het is zelfs niet uit te sluiten dat de (statelijke) aanvallers hier specifiek op uit waren (zeker ook gezien de combinatie van sabotage en spionage). Welke vitale aanbieders dit zijn en of dit ook een verstorend effect heeft op de continuïteit van **vitale processen** is niet goed in te schatten, maar het kan zeker niet worden uitgesloten.

Tabel 8 Scorekaart scenario aanval Cloud Service Provider

Thema	**Cyberdreigingen**	
Dreigingscategorie	Aantasting functioneren internet	
Scenario	Aanval Cloud Service Provider	
Scenariotoelichting	Aanval op een Cloud Service Provider waarbij zowel sprake is van data exfiltratie als sabotage (interne DDoS in een datacentrum in Nederland). Nederlandse gebruikers worden getroffen. Er zijn sterke vermoedens dat er een statelijke actor achter de aanval zit.	
Waarschijnlijkheidsbeoordeling (binnen 5 jaar)		**Toelichting**
Waarschijnlijkheid:	D	Gebeurtenissen zijn voorstelbaar en er zijn aanwijzingen dat dergelijke aanvallen gebeuren in de wereld. Niet ondenkbaar dat het zich ook tegen Nederland zou kunnen richten. Het is lastig om hier goede maatregelen tegen te nemen.
Beoordeling gevolgen (impact)		

Veiligheidsbelang	Criterium	Score	Toelichting
Territoriaal	1.1 Grondgebied	0	Niet van toepassing
	1.2 Internationale positie	0	Niet van toepassing: er worden met name Nederlandse klanten getroffen, er zullen dus minder snel verwijten richting Nederland gemaakt worden. Wel kan dit de internationale discussie over statelijke actoren op gang komen n.a.v. dit incident. Hoe de Nederlandse overheid hierop acteert kan invloed hebben op de discussie.
	1.3 Digitale ruimte	E	Het is zeer voorstelbaar dat in een dergelijk scenario ook vitale aanbieders geraakt worden. Vanwege de moedwilligheid van deze aanval is het zelfs voor de hand liggend dat zij ook doelwit zijn en het is lastig om hier goed tegen te weren. De omvang kan ook aanzienlijk zijn omdat door raamaanbestedingen en beperkt aantal partijen waarvan in de regel diensten worden afgenomen het regelmatig voorkomt dat bijvoorbeeld overheidspartijen van dezelfde CSP diensten afnemen. Het is dan ook niet ondenkbaar dat deze diensten vanuit het zelfde datacentrum worden geleverd.
	1.4 Bondgenootschappelijk grondgebied	0	Niet van toepassing
Fysiek	2.1 Doden	A	Het is niet ondenkbaar dat er slachtoffers vallen door de gevolgverstoringen in de samenleving. Het ligt erg aan de specifieke organisaties die geraakt zullen worden en of er daardoor ook bepaalde processen verstoord raken (in de zorg, het verkeer etc.). Maar er zullen zeker problemen ontstaan waarbij dodelijke incidenten kunnen optreden. *A met bovengrens B (vanwege potentie op verstoring vitale processen)*
	2.2 Ernstig gewonden en chronisch zieken	A	Het is niet ondenkbaar dat er ernstige gewonden vallen door de gevolgverstoringen in de samenleving. Het ligt erg aan de specifieke organisaties die geraakt zullen worden en of er daardoor ook bepaalde processen verstoord raken (in de zorg, het verkeer etc.). Maar er zullen zeker problemen ontstaan waarbij incidenten met ernstig gewonden kunnen optreden. *A met bovengrens B (vanwege potentie op verstoring vitale processen)*
	2.3 Gebrek primaire levensbehoeften	0	De duur van de verstoring is voor de meeste gebruikers relatief kort. Als vitale processen verstoord raken zullen deze mogelijk (tijdelijk) gaan uitwijken naar een andere CSP om de duur van de verstoring te beperken (dit moet wel al voorbereid zijn). De verwachting is dan ook dat er geen lichamelijk lijden zal ontstaan vanuit gebrek aan primaire levensbehoeften.

Veiligheidsbelang	Criterium	Score	Toelichting
Economisch	3.1 Kosten	B	Er zal flink wat financiële schade optreden bij getroffen bedrijven, maar vanwege de relatief korte duur zal dat met name sectoren treffen waarbij de omzet niet in de dagen erna ingehaald kan worden. Waar de schade precies optreedt is moeilijk in te schatten, maar uitgaande van een verlies van 2%-5% van de NLe economie per dag is de verwachting dat het denkbaar is dat het meer dan 50 miljoen betreft (vergelijking met bijvoorbeeld de aswolk van de IJslandse vulkaan waarbij er alleen al bij KLM 10 miljoen schade was per dag).
	3.2 Aantasting vitaliteit	0	Niet van toepassing
Ecologisch	4.1 Aantasting natuur en milieu	0	Niet van toepassing
Sociaal-politiek	5.1 Verstoring dagelijks leven	B	Het is denkbaar dat 3 à 4 indicatoren beperkt geraakt worden. **Onderwijs:** sommige instellingen kunnen worden geraakt, niet in grote mate. **Maatschappelijke voorzieningen / bereikbaarheid:** afhankelijk van type organisaties die geraakt worden kunnen bijvoorbeeld OV bedrijven of verkeerssystemen problemen ondervinden. Ook in de zorg kunnen mogelijk bepaalde activiteiten tijdelijk geen doorgang vinden. Ook andere maatschappelijke voorzieningen kunnen hier mee te maken krijgen maar dit zal niet op zeer grote schaal leiden tot het niet kunnen gebruik maken van maatschappelijke voorzieningen leiden **Virtuele bereikbaarheid:** kan ook worden geraakt (bepaalde systemen), maar kleine schaal. **Noodzakelijke aankopen:** er zullen effecten zijn bij winkels, maar het is de verwachting dat dit niet of nauwelijks leidt tot het niet kunnen doen van noodzakelijke aankopen.
	5.2 Aantasting democratische rechtsstaat	A	Vanwege sterke vermoeden van een statelijke actor is het niet volledig uit te sluiten dat zij beogen de samenleving en democratische rechtstaat te ontwrichten, maar dat is niet bewezen. Het belemmeren van functioneren is niet structureel, maar wel van toepassing.
	5.3 Sociaal-maatschappelijke impact	B	Er zal sprake zijn van angst, onrust en onzekerheid over wat er verder nog kan gebeuren (met name ook omdat het zich specifiek tegen NL doelwitten richt). Door de toenemende aandacht voor en bewustzijn over cyberaanvallen en de afhankelijkheid van digitale systemen zal er veel aandacht in de media en ook op sociale media zijn. Afhankelijk van eventuele informatie (of geruchten) over een specifieke statelijke actor kan polarisatie toenemen (zeker als dit inhaakt op bestaande spanningen of geopolitieke omstandigheden).

Veiligheidsbelang	Criterium	Score	Toelichting
Internationale rechtsorde en stabiliteit	6.1 Staatssoevereiniteit, vreedzame co-existentie en vreedzame geschillenbeslechting	A	Dit criterium is van toepassing want het betreft een aanval van een statelijke actor (infiltratie, sabotage, blokkeren systemen), hoewel attributie lastig is. Het is geen geweldsconflict en het is ook niet waarschijnlijk dat het een normdrager betreft. Er is momenteel nog geen internationaal wettelijk kader op dit vlak, wel *non binding* norms vanuit de UNGGE.
	6.2 Mensenrechten	0	Niet van toepassing
	6.3 Internationaal financieel-economisch bestel	0	Niet van toepassing
	6.4 Multilaterale instituties	A	Het criterium is van toepassing omdat niet uitgesloten kan worden dat bijvoorbeeld ook internationale organisaties in Nederland, zoals het Internationaal Strafhof geraakt kunnen worden. Er is echter in het scenario geen expliciete aanleiding voor concrete impact op dit vlak.
	6.5 Instabiliteit rondom Koninkrijk/EU	0	Niet van toepassing

3.3.3 Wild-card-scenario sabotage DNSSEC

Zoals ook benoemd in de ANV Verkenning uit 2018 [35] is het Domain Name System (DNS) één van de belangrijkste diensten voor het internet. Het is een systeem en netwerkprotocol dat host-namen in tekst (leesbaar voor mensen) vertaalt naar IP-adressen (bruikbaar voor machines) en omgekeerd. Vrijwel alle vormen van internetgebruik (particulier, organisaties en specifieke internetdiensten) zijn afhankelijke van DNS. [36]

Het DNS is een hiërarchisch systeem dat bestaat uit de root DNS, top-level domeinen (zoals .com en .nl), secundaire domeinen (bijvoorbeeld overheid.nl), etc. Hierin is de root DNS de hoogste hiërarchische laag, die volgens een gestandaardiseerd vraag-antwoord protocol doorverwijzingen geeft naar DNS data in lagere hiërarchische lagen.

Sinds 2010 is DNS data in de root DNS beveiligd middels het DNSSEC (Domain Name System Security Extensions) protocol. DNSSEC wordt oorspronkelijk gebruikt om DNS spoofing te voorkomen, maar wordt de laatste jaren ook steeds meer gebruikt als security bouwblok voor het waarborgen van de authenticiteit en integriteit van bijvoorbeeld e-mails en website certificaten.
Dit beveiligingsprotocol waarborgt dat de authenticiteit en integriteit van DNS records gevalideerd kan worden.

De manier waarop DNS en DNSSEC is ingericht, is kenmerkend voor hoe het internet is opgezet en wordt beheerd. Er is geen centraal beheer over DNS, maar het functioneert op basis van vertrouwens-mechanismen. Dit past ook bij de kernwaarden van het internet (*Internet Invariants*): [37]

- *Global reach, integrity;*
- *general purpose;*
- *supporting innovation without requiring permission;*
- *accessible;*
- *interoperability and mutual agreement;*
- *collaboration;*
- *reusable (technology) building blocks;*
- *no permanent favourites.*

Er zijn al langer bewegingen gaande die, langzaam maar zeker, deze waarden onder druk zetten. Dit heeft onder andere te maken met grote commerciële belangen van techgiganten en de manier waarop zij hun technologie ontwikkelen. Ook geopolitieke belangen spelen een rol, waarbij sommige landen meer grip willen krijgen op het gebruik van Internet in hun regio. Hoewel deze bewegingen niet direct het functioneren van het internet belemmeren, legt het wel een aantal kwetsbaarheden bloot. Dit zou ook door bepaalde gebeurtenissen verder kunnen escaleren en dat is wat met dit wild-card-scenario getracht wordt in

35 van Ruijven, Duijnhoven, Overeinder, Akkerhuis, "ANV Verkenning t.b.v. de risicocategorie Aantasten functioneren Internet".

36 Wouter C.A. Wijngaards, Benno J. Overeinder, "Securing DNS: Extending DNS servers with a DNSSEC validator," IEEE Security & Privacy 7, no. 5 (oktober 2009): 36-43, 10.1109/MSP.2009.133.

37 Internet Society, "Internet Invariants: What Really Matters".

beeld te brengen. De gebeurtenissen die worden beschreven in dit scenario kennen wellicht een zeer lage waarschijnlijk (o.a. vanwege de zware beveiliging van de *Root Zone KSK*), maar wanneer zoiets gebeurt dan zal dit vermoedelijk wel tot grote onrust en problemen in de internationale internet *community* (en politiek) veroorzaken.

Aanvullende achtergrond DNSSEC

De validatie van DNS records wordt mogelijk gemaakt door het toevoegen van een digitale handtekening, gebaseerd op *public key cryptography*, aan een DNS record. Aan de basis van DNSSEC ligt de *Root Zone Key Signing Key (KSK)*, een cryptografische sleutel. Die '*master' key* fungeert als een cryptografische vertrouwensbron ('*trust anchor*'), die het startpunt is voor het valideren van DNSSEC data. Vanaf deze *trust anchor* wordt, conform het DNSSEC protocol, via stapsgewijze opvraging van DNS sleutels een cryptografische '*chain of trust*' gemaakt naar de DNS data in lagere hiërarchische niveaus van het DNS.

ICANN (Internet Corporation for Assigned Names and Numbers) is de organisatie die het Internet *addressing & naming system* coördineert. De organisatie IANA *(Assigned Numbers Authority)*, die verbonden is aan ICANN, beheert ook de Root Zone KSK waar DNSSEC op gebaseerd is. De root zone KSK sleutel is opgeslagen in specifieke cryptografische apparatuur die aanwezig is op twee beveiligde locaties in de VS (één aan de Oostkust en één aan de Westkust). Sinds de invoering van DNSSEC in 2010 is de key één keer vervangen (in 2018). Dit was een spannend moment omdat het nog nooit eerder gedaan was en dit nogal wat voorbereiding vergt.

De Root Zone KSK is zwaar beveiligd en de toegang tot de kluis waar deze in is opgeslagen is beperkt tot een selecte groep vertegenwoordigers vanuit verschillende regio's.[38] Er moeten altijd meerdere van deze vertegenwoordigers aanwezig zijn om de ruimte te kunnen betreden en ook de sleutels om de ruimtes te kunnen betreden zijn streng beveiligd.

Bouwstenen

In Tabel 9 is het wild-card-scenario weergegeven aan de hand van factoren en actoren.

Tabel 9 Factoren en actoren wild-card-scenario sabotage DNSSEC

Oorzaak	Actor	Motief	Element	Middelen
Moedwillig	Statelijke actoren	(Geo-) Politieke doelstelling	DNS (rootservers, name servers, DNS operators)	Fysieke aantasting (explosie, kabel stuk, etc.)
			Vertrouwens-diensten (e.g. certificaten, public key infrastructure)	...

[38] Root Zone KSK Operator Policy Management Authority, "DNSSEC Practice Statement for the Root Zone KSK Operator," IANA (4 november 2020), https://www.iana.org/dnssec/procedures/ksk-operator/ksk-dps-20201104.html.

Tabel 9 Factoren en actoren wild-card-scenario sabotage DNSSEC (vervolg)

Aard van de aantasting	Getroffenen (direct)	Doordringingsgraad	Duur
Aantasting van beschikbaarheid	Digitale dienstverleners	Merendeel van de betreffende categorieën is getroffen is getroffen (>50%)	Half jaar of langer

Verhaallijn

Kwaadwillenden (vermoedelijk met een link naar een statelijke actor) zijn in staat om de *DNS Root Zone Key Signing Key* (KSK) te vernietigen (op beide locaties waar deze is opgeslagen). De operatie wordt zo uitgevoerd dat deze niet direct wordt opgemerkt, dit zal pas gebeuren als de Root Zone KSK nodig is voor een zogenaamde '*DNSSEC Root Signing Ceremony*' waarbij de Root Zone KSK wordt gebruikt om operationeel gebruikte DNSSEC keys te ondertekenen en te verifiëren. Dit gebeurt ongeveer eens per kwartaal.

Het vernietigen van de sleutels heeft geen onmiddellijke impact op de werking van het internet. Het zorgt ervoor dat er geen nieuwe *operational keys* kunnen worden getekend. Dit leidt er weer toe dat er na verloop van tijd geen *operational keys* meer zijn, waardoor de integriteit van DNS data niet meer gevalideerd kan worden. Het zorgt er dus effectief voor dat het beveiligingsprotocol van het DNS systeem, DNSSEC, niet meer werkt. Dit is problematisch omdat steeds meer internetapplicaties gebruik maken van DNSSEC.

Doordat DNSSEC niet meer werkt, worden allerlei ernstige kwetsbaarheden die waren gemitigeerd in een keer weer actueel (cache-poisoning, DNS-spoofing, rogue Internet certificates, etc.). Het gebruik van DNSSEC neemt in de laatste jaren snel toe [39] (Bijvoorbeeld veruit het merendeel van de TLD zijn DSNSEC signed [40]), dus de problemen kunnen groot zijn. Dat veroorzaakt veel onrust in de internet community en bij cybersecurity experts. Hoewel de samenleving hier niet direct hinder van zal ondervinden, is er een groot risico dat allerlei kwaadwillende actoren hier vroeg of laat misbruik van gaan maken en er in de loop der tijd dus een enorme hoeveelheid cyber aanvallen zal gaan ontstaan richting allerlei doelwitten.

Het herstellen van DNSSEC betekent in feite het volledig opnieuw opbouwen van het systeem en dit heeft enorm veel voeten in de aarde. Dit zal meerdere jaren in beslag nemen. Terwijl hier in de ICANN community druk aan wordt gewerkt, klinken er ook steeds meer geluiden dat dit wellicht een goede aanleiding is om de manier waarop het internet is ingericht en wordt beheerd eens op de schop te nemen. Vanuit verschillende landen wordt aangegeven dat het misschien wel goed zou zijn om niet alles meer in de VS de concentreren en om ook wat meer betrokkenheid uit andere delen van de wereld toe te voegen. Hiermee laait de geopolitieke ruzie over internet governance weer volledig op.

Inschatting impact op nationale veiligheid

Geraadpleegde experts zijn het er over eens dat de waarschijnlijkheid dat kwaadwillenden in staat zijn om DNS *Root Zone Key Signing Key* (KSK) te vernietigen op beide locaties waar deze is opgeslagen extreem klein is, en zelfs als dat lukt zijn er ook nog 5 mensen met back-up keys waarmee alles hersteld kan worden.

Toch is dit scenario interessant omdat het wel een voorbeeld is van een gebeurtenis die de waarden van het open internet kan aantasten. De gebeurtenis zou de doodsteek zijn voor DNSSEC en dan zal er een hernieuwde discussie ontstaan over alternatieve technologie, inrichting en standaardisatie. De kans is dan groot dat de huidige consensus in de Tunis Agenda [41] onderuit gehaald wordt. Dat betekent dat het multi-stakeholder model dat de basis vormt voor het huidige functioneren van het internet en de manier waarop het decentraal gemanaged wordt, onder druk komt te staan. Er zijn staten die al langer pleitten voor nieuwe governance modellen voor het internet en een gebeurtenis zoals deze kan daarbij ook andere landen over de streep halen.

39 Berry van Halderen en Roland van Rijswijk-Deij, "Supporting DNSSEC Key Signing Ceremonies," NLNet Labs (1 december 2020), https://blog.nlnetlabs.nl/supporting-dnssec-key-signing-ceremonies/.

40 ICANN Research, "TLD DNSSEC Report," http://stats.research.icann.org/dns/tld_report/.

41 World summit on the information society, Tunis Agenda for the Information Society, WSIS-05/TUNIS/DOC/6(Rev. 1)-E (november 2005), https://www.itu.int/net/wsis/docs2/tunis/off/6rev1.html.

De Nederlandse economie en samenleving is gebaat bij een≈open digitale samenleving en wij spelen daar een vooraanstaande rol in. Als de internationale consensus wegvalt heeft dat invloed op Nederland als digitaal handelsland, hiermee kan op termijn de vitaliteit van onze economie en het verdienvermogen onder druk komen te staan. Dat zal niet direct gebeuren, maar op termijn heeft het grote invloed op de digitale sector.

Internationaal staat ook de vrijheid van individuen en mensenrechten op het spel. Je krijgt een ander soort internet waarin overheden meer invloed hebben en dat kan een gevaar zijn voor burgers en maatschappelijke organisaties binnen sommige regimes.

Op de kortere termijn zal na een dergelijke gebeurtenis vooral onrust ontstaan in de internet community. Er kunnen wel wat problemen ontstaan door het wegvallen van DNSSEC, maar veel kan ook wel weer opgevangen worden. Er komt geen onderbreking van het functioneren van het internet, maar er kan wel een verlies van vertrouwen in de internet infrastructuur ontstaan al is het de vraag in hoeverre de onrust zich ook in de maatschappij zal verspreiden. Veel mensen zullen er niet echt iets van merken.

3.4 Beschouwing

De ontwikkelingen binnen deze dreigingscategorie en de uitkomst van de analyse bevestigen opnieuw het beeld dat het internet een robuuste infrastructuur kent en dat incidenten in de praktijk vaak een relatief beperkte duur en omvang hebben. Toch kan de impact van incidenten een ernstig gevolg hebben voor de nationale veiligheid omdat internet en internetdiensten een steeds belangrijkere rol in maatschappelijke processen spelen. Ook de dominante rol en van grote aanbieders van internetdiensten speelt hierbij een rol. Bij verstoringen van de dienstverlening van dergelijke techgiganten zullen de effecten op heel veel plekken in de samenleving merkbaar zijn. Een belangrijk inzicht is dat het heel erg moeilijk is om op voorhand in te schatten wat er allemaal mis zal gaan bij dit type verstoringen en dat maakt het ook erg lastig om hier goed op voorbereid te zijn. Het complexe en veranderlijke karakter van het internetlandschap draagt hier aan bij.

Daarentegen is de waarschijnlijkheid van dit type gebeurtenis vrij hoog. Incidenten (moedwillig en niet-moedwillig) gebeuren continu en overal en door de toenemende complexiteit en vernetting van systemen zijn ze steeds lastiger te verhelpen omdat er onverwachte en onbekende complicaties kunnen optreden.

De beschreven ontwikkelingen en het wild-card-scenario laten tevens zien dat geopolitieke en economische belangen een belangrijke rol spelen in de manier waarop naar het internet en toekomstige technologische ontwikkelingen wordt gekeken, waardoor de manier waarop het internet is ingericht en de onderliggende waarden onder druk komen te staan. Dit zal niet direct het functioneren van het internet belemmeren, maar kan wel op termijn serieuze negatieve effecten hebben voor Nederland als digitale economie.

4. Dreigingscategorie verstoring cyber-fysieke systemen

Deze dreigingscategorie richt zich op de potentiële gevolgen van incidenten met zogenaamde cyber-fysieke systemen. Het gaat hierbij om digitale systemen die worden gebruikt om fysieke processen aan te sturen. [42] Hierbij gaat het enerzijds om zogenoemde Industriële Controle Systemen genoemd. ICS zijn onderdeel van de operationele technologie (OT) en worden in veel sectoren gebruikt om uiteenlopende processen aan te sturen, zoals energiesystemen, drinkwaterdistributie, het bedienen van pompen, bruggen en sluizen, beveiligingssystemen of chemische industrie-processen. Naast ICS kunnen fysieke processen ook verstoord raken door incidenten die betrekking hebben op IT systemen die mogelijk niet technisch gekoppeld zijn aan operationele technologie, maar waarbij wel een functionele afhankelijkheid bestaat (bijvoorbeeld IT systemen die gebruikt worden voor logistieke planning of het uitvoeren van financiële transacties), waardoor verstoring wel kan leiden tot belemmeringen voor het fysieke proces. Hierbij is het ook van belang om aandacht te hebben voor de afhankelijkheden van systemen van ketenpartners of toeleveranciers. Een verstoring kan ook ontstaan vanuit problemen die een oorsprong hebben bij een andere organisatie, maar waarbij vanwege technische of functionele relaties de effecten ook doordringen tot de eigen organisatie. Omdat ICS ook in veel vitale processen een belangrijke rol spelen is er een nauwe relatie tussen deze dreigingscategorie en het thema bedreiging vitale infrastructuur. Hoewel het in deze categorie gaat over gebeurtenissen die leiden tot verstoring van cyber-fysieke systemen is het belangrijk om bewust te zijn van de samenhang met een aantal andere fenomenen. Statelijke actoren en ook criminele groeperingen voeren ook acties uit die niet zozeer gericht zijn op sabotage, maar om informatie te verkrijgen (spionage), om verwarring te scheppen (hybride campagnes) of om voorbereidingen te treffen om tot actie te kunnen overgaan als dat opportuun is.

4.1 Relevante ontwikkelingen

Toename van gespecialiseerde ICS malware

De aanval op een Iraanse nucleaire installatie met het Stuxnet virus in 2010 [43] is een van de eerste bekende voorbeelden van een gerichte aanval op ICS. Dit incident wordt nog steeds vaak gebruikt om het belang van deze dreiging te onderstrepen. Een ander bekend voorbeeld is de aanval met de malware BlackEnergy gericht op de elektriciteitsvoorziening in Oekraïne (2015). [44] Meer recente voorbeelden van malware die zich specifiek op ICS richtten zijn o.a. de LockerGoga Ransomware [45] en EKANS [46] die beide vanaf 2019 gesignaleerd worden. Experts maken zich zorgen dat aanvallers over steeds meer kennis van ICS beschikken. Ook waarschuwt de FBI in 2022 dat de daders

42 Edward A. Lee, "Cyber physical systems: Design challenges," *11th IEEE international symposium on object and component-oriented real-time distributed computing* (ISORC) (mei 2008): 363-369, 10.1109/ISORC.2008.25.

43 Kim Zetter, "An Unprecedented Look at Stuxnet, the World's First Digital Weapon," Wired (3 november 2014), https://www.wired.com/2014/11/countdown-to-zero-day-stuxnet.

44 Kim Zetter, "Inside the Cunning, Unprecedented Hack of Ukraine's Power Grid," Wired (3 maart 2016), https://www.wired.com/2016/03/inside-cunning-unprecedented-hack-ukraines-power-grid/.

45 Andy Greenberg, "A guide to LockerGoga, the Ransomware Crippling Industrial Firms," Wired (25 maart 2019), https://www.wired.com/story/lockergoga-ransomware-crippling-industrial-firms/.

46 Charlie Osborne, "This is how EKANS ransomware is targeting industrial control systems," ZDNet (2 juli 2020), https://www.zdnet.com/article/this-is-how-ekans-ransomware-is-targeting-industrial-control-systems/.

achter de Triton aanval tegen een petrochemische fabriek in Saudi Arabië in 2017 [47] nog steeds een relevante dreiging vormen voor de ICS van vitale infrastructuur. [48] Naast specifieke malware kunnen verstoringen van cyber-fysieke systemen namelijk ook op minder geavanceerde manieren tot stand komen, bijvoorbeeld door een insider, of misbruik van kwetsbaarheden om steeds dieper tot systemen door te dringen. [49] De poging om het drinkwater van een Amerikaans drinkwaterbedrijf in Florida te vergiftigen in 2021 [50] is een spraakmakend voorbeeld van een cyberaanval gericht op sabotage van cyber-fysieke systemen.

Toename van ransomware aanvallen in relatie tot ICS

Er is in algemene zin een toename van het aantal aanvallen met ransomware [51], maar deze trend lijkt zich ook specifiek te manifesteren in ICS [52], al is het soms meer opportunisme vanuit de aanvallers of is het effect op de ICS vooral een neveneffect. De NotPetya (2017) [53] en WannaCry(2017) [54] aanvallen gelden als bekende voorbeelden van aanvallen waarbij de effecten zich snel over heel veel verschillende sectoren verspreidden en waardoor verschillende bedrijven, waaronder Maersk (NotPetya) en verschillende ziekenhuizen in het VK (WannaCry) genoodzaakt waren om (een deel van) hun operationele processen stil te leggen.

In Nederland waren er in 2021 in verschillende supermarktketens enige tijd nauwelijks kaas- en andere zuivelproducten beschikbaar door een ransomware aanval op een logistiek bedrijf dat de distributie voor deze producten verzorgt. [55] Bij een ransomware aanval op het Amerikaanse Colonial Pileline besloot het bedrijf uit voorzorg de hele operatie stil te leggen omdat het op het moment van de aanval niet bekend was hoe diep de aanvallers in de systemen waren doorgedrongen en of er een mogelijkheid was dat ze daadwerkelijk de operationele processen zouden kunnen saboteren. [56]
Als gevolg van het stilleggen van de operatie ontstond er maatschappelijke onrust en kwam er een run op benzine, waardoor er al snel tekorten ontstonden.

Onderscheid tussen OT en IT is aan het vervagen (convergentie)

Als gevolg van processen van digitalisering vinden steeds meer IT componenten hun weg naar OT omgevingen, waardoor het onderscheid tussen IT en OT (inclusief ICS) aan het vervagen is. [57] Digitalisering biedt namelijk veel kansen voor het vergroten van efficiency en effectiviteit in OT systemen. Maar met deze integratie worden ook IT kwetsbaarheden en risico's overgebracht naar OT omgevingen. Dit wordt als een groot risico gezien omdat OT systemen niet makkelijk op dezelfde manier te beveiligen zijn. [58] Zo is de levensduur van ICS doorgaans veel langer dan van een IT systeem, waardoor het aanpassen van de systemen ingewikkelder is. [59]

Daarbij is bij veel organisaties het beheer van IT en OT in gescheiden teams belegd, waardoor er ook weinig van elkaar kan worden geleerd. OT is dus vaak kwetsbaar en in combinatie met een toenemende dreiging van met name statelijke actoren die erop gericht zijn om sabotage van vitale infrastructuur mogelijk te maken [60] is dit voor experts reden tot zorg.

47 Martin Giles, "Triton is the world's most murderous malware, and it's spreading," MIT Technology Review (5 maart 2019), https://www.technologyreview.com/2019/03/05/103328/cybersecurity-critical-infrastructure-triton-malware/.

48 FBI Cyber Division, "TRITON Malware Remains Threat to Global Critical Infrastructure Industrial Control Systems (ICS)," 24 maart 2022, https://www.ic3.gov/Media/News/2022/220325.pdf.

49 Waterfall publiceerde in 2018 analyse van kwetsbaarheden met daarin een top 20 van cyber aanvalstechnieken gericht op ICS: Waterfall, "The Top 20 Cyber Attacks on Industrial Control System," Waterfall Security (2018), https://waterfall-security.com/20-attacks/.

50 Andy Greenberg, "A Hacker Tried to Poison a Florida City's Water Supply, Officials Say," Wired (8 februari 2021), https://www.wired.com/story/oldsmar-florida-water-utility-hack/.

51 Amiah Taylor, "There's a huge surge in hackers holding data for ransom, and experts want everyone to take these steps," Fortune (17 februari 2022), https://fortune.com/2022/02/17/ransomware-attacks-surge-2021-report/.

52 Benoit Bouffard en Leo Pernet-Mugnier, "What are the trends and challenges in industrial cybersecurity in 2021?," RiskInsight (oktober 2021), https://www.riskinsight-wavestone.com/en/2021/10/what-are-the-trends-and-challenges-in-industrial-cybersecurity-in-2021/; Shannon Williams, "Ransomware topped ICS and OT threats in 2021 – report," Securitybrief (3 maart 2022), https://securitybrief.co.nz/story/ransomware-topped-ics-and-ot-threats-in-2021-report.

53 Andy Greenberg, "The Untold Story of NotPetya, the Most Devastating Cyberattack in History," Wired (22 augustus 2018), https://www.wired.com/story/notpetya-cyberattack-ukraine-russia-code-crashed-the-world/.

54 Lily-Hay Newman, "The Ransomware Meltdown Experts Warned About Is Here," Wired (12 mei 2017), https://www.wired.com/2017/05/ransomware-meltdown-experts-warned/.

55 NOS, "'Kaas-hack' opgelost, ging om gijzelsoftware," NOS Nieuws (12 april 2021), https://nos.nl/artikel/2376425-kaas-hack-opgelost-ging-om-gijzelsoftware.

56 W. Turton en K. Mehrotra, "Colonial Pipeline Cyber Attack: Hackers Used Compromised Password," Bloomberg (4 juni 2021), https://www.bloomberg.com/news/articles/2021-06-04/hackers-breached-colonial-pipeline-using-compromised-password#xj4y7vzkg.

57 "ICS/SCADA," Nationaal Cyber Security Centrum, https://www.ncsc.nl/onderwerpen/ics.

58 Chuck Brooks, "3 Key Cybersecurity Trends To Know For 2021 (and On ...)," Forbes (12 april 2021), https://www.forbes.com/sites/chuckbrooks/2021/04/12/3-key-cybersecurity-trends-to-know-for-2021-and-on-/?sh=7d4a08374978.

59 Iid.

60 Ibid.

4.2 Overzicht van mogelijke actoren en factoren

Hoewel er rondom ICS en cyber-fysieke systemen doorgaans vooral veel aandacht is voor de dreiging van moedwillige aanvallen, kan ook technisch of menselijk falen leiden tot verstoring. In het overzicht van relevante factoren en actoren moet dus ook met deze verschillende **oorzaken** rekening worden gehouden. Het dreigingslandschap is gevarieerd en er zijn uiteenlopende **actoren** en **motieven** die een rol kunnen spelen bij incidenten met betrekking tot cyber-fysieke systemen. De mogelijke (combinatie van) **middelen** waarmee een verstoring tot stand wordt gebracht zijn dezelfde typen middelen als voor andere cyberdreigingen en ook de **aard van de aantasting** kan op dezelfde manier getypeerd worden. Als het gaat om de impact is het ook bij deze categorie belangrijk om aandacht te hebben voor mogelijke supply chain incidenten (waarbij een aanval op een organisatie tot stand komt via een leverancier of aanbieder van digitale diensten. Om die reden kan het relevant zijn om onderscheid te maken tussen direct en indirect **getroffenen**. De omvang en ernst van een aantasting van het functioneren van het Internet is lastig in concrete factoren uit te drukken omdat dit heel er afhangt van het type situatie en proces dat verstoord raakt. Verstoringen van ICS kunnen zich beperken tot één of enkele locatie, maar bij verstoringen die veroorzaakt worden door bijvoorbeeld malware in veelgebruikte software kan het zich ook over veel verschillende organisaties verspreiden. Om die reden is de **doordringingsgraad** van de verstoring een andere relevante factor, net als de duur van de verstoring die kan variëren van een of enkele dagen tot maanden of zelfs langer. Deze factoren zijn van invloed op de ernst van de impact.

Tabel 10 Factoren en actoren dreigingscategorie verstoring cyber-fysieke systemen

Oorzaak	Actor	Motief	Middelen	Aard van de aantasting
Technisch falen	Criminelen [61]	Economisch gewin	Distributed Denial of Service (DDoS)	Aantasting van beschikbaarheid
Menselijk falen	Statelijke actoren	Ideologische doelstelling	Misconfiguratie	Aantasting van integriteit
Moedwillig	Terroristen	(Geo-) politieke doelstelling	Fysieke aantasting (explosie, kabel stuk, etc.)	Aantasting van betrouwbaarheid
	Cyber-vandalen en scriptkiddies	Ego, profilering of wraak	Malware infectie (inclusief ransomware)	
	Hacktivisten		Misbruik van kwetsbaarheden	
	Interne actoren		Social engineering (incl. phishing)	
	Cyber-onderzoekers		....	
	Private organisaties			

[61] Dit omvat zowel autonome criminele samenwerkingsverbanden, dienstverleners van zgn. 'cybercrime-as-a-service' en individuele cybercriminelen

Tabel 10 Factoren en actoren dreigingscategorie verstoring cyber-fysieke systemen (vervolg)

Getroffenen (direct)	Getroffenen (keteneffecten)	Doordringingsgraad	Duur
Vitale aanbieders	Vitale aanbieders	Klein deel van de betreffende categorieën is getroffen (<10%)	Tot 1 dag
Rijksoverheid	Rijksoverheid	Aanzienlijk deel van de betreffende categorieën is getroffen (10-50%)	2 tot 6 dagen
Digitale dienstverleners	Digitale dienstverleners	Merendeel van de betreffende categorieën is getroffen (>50%)	1 tot 4 weken
Topsectoren	Topsectoren		1 tot 6 maanden
Kennis instellingen	Kennis instellingen		Half jaar of langer
Overige organisaties (incl. gemeenten, veiligheidsregio's, MKB)	Overige organisaties (incl. gemeenten, veiligheidsregio's, MKB)		Onherstelbaar
Burgers	Burgers		

4.3 Scenario's

In de selectie van dreigingsscenario's voor de huidige analyse is ervoor gekozen om vooral op de dreiging van moedwillige aanvallen met betrekking tot cyber-fysieke systemen te richten. Het is niet uit te sluiten dat er niet-moedwillige verstoringen ontstaan, maar de focus op moedwillige dreigingen is in lijn met de toenemende aandacht hiervoor bij analisten en experts. Naast het eerder door het ANV uitgewerkte scenario 'Collateral Damage' dat is geïnspireerd op de grootschalige incidenten NotPetya en WannaCry, is er voor deze analyse gekozen om een scenario uit te werken van een gerichte aanval vanuit een statelijke actor op een industrieel proces, met ernstige fysieke impact.

Reguliere Scenario's
Cyberaanval ICS – chemische sector
Collateral damage

4.3.1 Scenario cyberaanval ICS - chemische sector

Het scenario betreft een cyberaanval door een staats-gelieerde hackersgroep op een chemische fabriek in Nederland. Via social engineering weten de aanvallers zich toegang te verschaffen en nemen daar de tijd om door te dringen tot de ICS van de fabriek. Op enig moment veroorzaken de aanvallers een chemisch incident waarbij een grote hoeveelheid ammoniak vrijkomt. Voor de effecten van de verspreiding van ammoniak wordt gebruik gemaakt van een scenario uit het thema zware ongevallen, waarin een ongeluk met een ammoniakopslag is uitgewerkt.

We maken hier gebruik van een grotendeels vergelijkbaar incident dat elders in de risicoanalyse wordt gebruikt om het risico van chemische ongevallen te analyseren.
De nadruk in deze analyse ligt op de oorzaak (digitale aanval vanuit een statelijke actor) en de denkbare gevolgen die dat met zich meebrengt. Welke staat er achter de aanval zit is in het scenario niet gespecifieerd al is wel met experts besproken dat het niet voor de hand ligt dat dit een EU lidstaat betreft of een NAVO bondgenoot. Verder zijn de capaciteiten om een dergelijke aanval uit te voeren vermoedelijk ook niet in alle landen beschikbaar.

Het scenario vormt enerzijds een aanvulling op de analyse van chemische incidenten binnen het thema zware ongevallen, omdat dergelijke incidenten ook veroorzaakt kunnen worden door een moedwillige aanval. De keuze voor een statelijke actor legt tevens een link met het thema internationale en militaire dreigingen omdat een dergelijke actie als een oorlogsdaad zal worden opgevat.
Dat statelijke actoren zich met digitale middelen toegang verschaffen tot systemen waarmee (vitale) processen worden aangestuurd is ook een bekende actie die als onderdeel van een hybride campagne kan worden ingezet, maar nog zonder dat de escalatie tot een fysiek incident zich daadwerkelijk manifesteert.

Tabel 11 Factoren en actoren scenario cyberaanval ICS - chemische sector

Oorzaak	Actor	Motief	Middelen [62]
Moedwillig	Statelijke actoren	(Geo-) politieke doelstelling	Fysieke aantasting (explosie, kabel stuk, etc.)
			Malware infectie (inclusief ransomware)
			Social engineering (incl. phishing)

[62] In de praktijk wordt vaak een combinatie van aanvalstechnieken gebruikt.

Tabel 11 Factoren en actoren scenario cyberaanval ICS - chemische sector (vervolg)

Aard van de aantasting	Getroffenen (direct)	Doordringingsgraad	Duur
Aantasting van integriteit	Overige organisaties (incl. gemeenten, veiligheidsregio's, MKB)	Klein deel van de betreffende categorieën is getroffen (<10%)	2 tot 6 dagen
			1 tot 4 weken

Bouwstenen

In Tabel 11 is het scenario weergegeven aan de hand van de factoren en actoren. De duur van de aantasting is uitgesplitst in enerzijds de duur van het effect van het chemische incident (enkele dagen) en anderzijds de duur van de aantasting van integriteit van de ICS van de betreffende organisatie, wat een stuk langer zal duren (systemen moeten worden opgeschoond en hersteld).

Verhaallijn

De voorbereiding: een digitale aanval om sabotage mogelijk te maken

Een staatsgelieerde hackersgroep heeft zich via een spear phising campagne toegang weten te verschaffen tot de kantoorautomatiseringsomgeving (IT) van een fabriek in de chemische sector. Omdat de aanval onopgemerkt blijft hebben ze tijd om te zoeken naar manieren om vanuit de kantooromgeving ook toegang te krijgen tot de industrial control systems in de operationele technologie (OT) omgeving van het bedrijf. Hoewel de IT-omgeving en de OT-omgeving gesegmenteerd is, bestaan er wel bepaalde verbindingen en deze hackers hebben genoeg verstand van zaken om deze verbindingen te lokaliseren en te gebruiken om de OT-systemen binnen te dringen. Hoe verder ze in de systemen komen, hoe meer kwetsbaarheden ze tegenkomen. Uiteindelijk zijn ze – nog altijd onopgemerkt – in staat om gespecialiseerde malware [63] te installeren waardoor ze de controle over verschillende operationele processen kunnen krijgen. Hiermee zijn ze er klaar voor om een fysiek incident te veroorzaken als dat voor hun opdrachtgevers opportuun is.

De escalatie: sabotage met een ernstig chemisch incident als gevolg [64]

Op een zomerse namiddag wordt via de procesbesturing een klep van een ammoniakopslag opengezet waardoor er in een tijdbestek van 10 minuten een grote hoeveelheid ammoniak vrij komt (het gaat om een drukopslag met 500 ton ammoniak). Omdat de aanvallers ervoor hebben gezorgd dat ook de veiligheidssystemen voor detectie en controle zijn gemanipuleerd wordt de lekkage niet direct opgemerkt. De vrijgekomen ammoniak verdampt direct en er ontstaat een giftige ammoniakwolk die zich snel met de wind mee verspreidt. De wolk verspreidt zich over het terrein en gaat richting de nabijgelegen woonwijk. Die woonwijk ligt op zo'n 300 meter van het concern en er wonen circa 3000 mensen. Vanwege het rustige en mooie weer zijn redelijk veel mensen buiten. Zij hebben wel de sirenes gehoord, maar zagen geen directe reden om naar binnen te gaan; het incident leek beperkt en relatief ver weg.

Er is uiteindelijk onvoldoende tijd voor evacuatie en veel mensen worden blootgesteld aan hoge ammoniak-concentraties. Er vallen enkele tientallen doden en honderden ernstig zieken (ademhalingsklachten). Daarbij zitten ook mensen die wel binnen waren, maar vanwege de hoge concentratie ammoniak toch slachtoffer zijn geworden. Politie en ambulances kunnen in het eerste uur het gebied niet in vanwege de hoge ammoniak-concentraties en ook het werk van de brandweer wordt bemoeilijkt door een tekort aan persoonlijke beschermingsmiddelen.

63 Bekende voorbeelden van malware specifiek gericht op industriële controle systemen zijn Stuxnet, LockerGoga, EKANS en BlackEnergy.

64 Afgeleid van het scenario Falen van opslagtank ammoniak uit het thema Zware ongevallen.

Ter plaatse heerst er chaos en er is al gauw sprake van angst en onrust, zowel onder de bevolking in het omringende gebied als op andere plekken in Nederland. Ook de media en politiek roeren zich. De verspreiding van de ammoniak leidt verder tot tijdelijke schade aan natuur en oppervlaktewater in het benedenwindse gebied. Een innamepunt voor drinkwaterbereiding wordt tijdelijk gesloten.

De nasleep

Tijdens het onderzoek naar het incident wordt al snel duidelijk dat er met de procesbesturing is geknoeid waardoor zowel de klep open kwam te staan én de detectiesystemen niet gewerkt hebben. Forensisch digitaal onderzoek laat zien dat er gebruik gemaakt is van malware die eerder in verband is gebracht met hackersgroepen uit land X. Dit lijkt er op te duiden dat hier sprake is van een directe aanval op Nederland vanuit een statelijke hoek. Er wordt direct een beraad georganiseerd met de minister president, de ministers van Defensie, Buitenlandse Zaken, Justitie en Veiligheid, en Binnenlandse Zaken en Koninkrijkrelaties, de veiligheidsdiensten en andere relevante partijen om de Nederlandse reactie (in samenspraak met bondgenoten) te bespreken.

Beoordeling van de impact en waarschijnlijkheid

Bij de beoordeling van de impact van het chemische incident (de ammoniakwolk) is gebruik gemaakt van de beoordeling zoals die is gedaan voor het oorspronkelijke scenario uit het thema Zware ongevallen. Binnen deze categorie hebben we met experts gekeken op welke criteria de aspecten die samenhangen met de digitale aanval en het moedwillige (statelijke) karakter van de gebeurtenissen impact hebben. Voor de waarschijnlijkheid geldt dat gekeken is naar de waarschijnlijkheid van de gebeurtenissen in het licht van het fenomeen dat in deze categorie centraal staat (een gerichte aanval op een fysiek proces in Nederland door een statelijke actor en met ernstige fysieke effecten).

Hoewel er aanwijzingen zijn dat statelijke actoren wereldwijd voorbereidingen treffen voor dit type aanvallen, zijn er op dit moment geen concrete aanwijzingen dat staten een reden hebben om een dergelijke aanval in Nederland ook daadwerkelijk uit te voeren, hoewel de huidige geopolitieke ontwikkelingen het mogelijk wel waarschijnlijker maken dat Nederland in een conflict betrokken raakt, waarbij actoren ook naar dit type middelen kunnen grijpen.

De impact van de gebeurtenissen in dit scenario zijn ernstig, er vallen doden en gewonden en er zal ook maatschappelijke angst, onrust en woede ontstaan. Maar de potentiële gevolgen die uit een dergelijk scenario volgen kunnen nog veel groter zijn, afhankelijk van de reacties vanuit Nederland en haar bondgenoten. Om hier een beeld van te krijgen verwijzen we naar de themarapportage internationale en militaire dreigingen.

Er wordt naar aanleiding van de gebeurtenissen in dit scenario geen impact op **vitale processen** verwacht, al is het wel belangrijk om in het oog te houden dat juist ook vitale processen doelwit kunnen zijn van dergelijke cyberaanvallen en sabotage-activiteiten.

Tabel 12 Scorekaart scenario cyberaanval ICS-chemische sector

Thema	**Cyberdreigingen**	
Dreigingscategorie	Verstoring cyber-fysieke systemen	
Scenario	Cyberaanval ICS - chemische sector	
Scenariotoelichting	Cyberaanval op chemieconcern, waarbij aanvallers via IT omgeving ook toegang verkrijgen tot industriële procescontrole systemen. Sabotage leidt tot het vrijkomen van een grote hoeveelheid ammoniak. Het blijkt een aanval van een statelijke actor te zijn en de vraag is hoe Nederland op deze aanval zal reageren.	
Waarschijnlijkheidsbeoordeling (binnen 5 jaar)		**Toelichting**
Waarschijnlijkheid:	B	Statelijke actoren zijn technisch gezien in staat om dit te doen en er zijn ook internationale voorbeelden waarbij iets vergelijkbaars gebeurd lijkt te zijn, maar het is op dit moment onwaarschijnlijk dat ze doelgericht een dergelijke aanval op een Nederlands doelwit zouden uitvoeren.
Beoordeling gevolgen (impact)		

Veiligheidsbelang	Criterium	Score	Toelichting
Territoriaal	1.1 Grondgebied	0	Niet van toepassing. Er zullen op het terrein van het chemieconcern wel opruimwerkzaamheden plaatsvinden.
	1.2 Internationale positie	A	Aanval is gericht op Nederland dus de verwachting is niet dat dit direct tot reacties tegen Nederland zal leiden (vanuit bondgenoten juist steun omdat Nederland slachtoffer is). Toch kan dit niet helemaal uitgesloten worden (bijvoorbeeld teruglopend toerisme of schade aan politieke betrekkingen). Reactie vanuit Nederland op dit incident kan tot tegenreacties leiden. Bijvoorbeeld openlijk attributie richting een andere staat, zou tot reacties kunnen leiden (zowel positief als negatief). Als Nederland al in een geopolitiek conflict verwikkeld is kan dit incident gebruikt worden om Nederland in negatief daglicht te zetten.
	1.3 Digitale ruimte	B	Het chemiebedrijf dat wordt aangevallen is geen vitale aanbieder en het betreft slechts één bedrijf. Er zit wel een politiek motief achter en de aanvallers hebben ongemerkt toegang verschaft en een incident kunnen veroorzaken.
	1.4 Bondgenootschappelijk grondgebied	0	Niet van toepassing. De aanval is op NL grondgebied.
Fysiek	2.1 Doden	B	Er vallen enkele tientallen slachtoffers
	2.2 Ernstig gewonden en chronisch zieken	C	Veel mensen die zijn blootgesteld aan de ammoniak hebben ademhalingsklachten (longschade) en/of oogirritatie. Het gaat om enkele honderden personen uit de woonwijk.
	2.3 Gebrek primaire levensbehoeften	B	Als een grote groep mensen (enkele honderden) acute zorg nodig heeft, kan dat meerdere dagen tot capaciteitsproblemen leiden.
Economisch	3.1 Kosten	A	Herstelkosten voor de IT/OT van het getroffen bedrijf ('slechts' opschonen of volledig opnieuw opbouwen zal invloed hebben op de kosten) en daardoor ook financiële schade (bedrijf zal tijdens herstelperiode waarschijnlijk (deels) stil komt te liggen), bestrijdings-kosten van effecten ammoniak in de omgeving (inzet hulpdiensten etc.) en gezondheidsschade (m.n. korte termijnbehandeling). Inschatting enkele tientallen miljoenen Euro's, waarbij de vraag is of het de 50 miljoen overschrijdt (bovengrens B). NB. Er zal n.a.v. een dergelijke aanval ook breder onderzoek opgezet worden (o.a. NCSC) naar mogelijk andere targets in de sector of zelfs andere Nederlandse sectoren, bedrijven zullen zelf acties gaan ondernemen en zoeken naar kwetsbaarheden maar die kosten zijn indirect en worden hier niet in meegenomen.
	3.2 Aantasting vitaliteit	0	Niet van toepassing

Veiligheidsbelang	Criterium	Score	Toelichting
Ecologisch	4.1 Aantasting natuur en milieu	A	Het milieu zal op kleine schaal aangetast worden maar de aantasting is kortdurend en maximaal 30 km².
Sociaal-politiek	5.1 Verstoring dagelijks leven	A	<10.000 mensen uit de getroffen woonwijk kunnen maximaal 1 à 2 dagen niet normaal in het getroffen gebied verblijven. Dit betekent dat zij voor korte tijd niet werk kunnen uitvoeren of onderwijs kunnen volgen.
	5.2 Aantasting democratische rechtsstaat	A	De aanval lijkt er niet op gericht zijn de democratische rechtsstaat aan te tasten, maar het is niet ondenkbaar dat een dergelijke aanval onderdeel is van een bredere campagne. De aanval zal naar verwachting geen tot weinig invloed hebben op het functioneren van de betreffende functiegroepen, maar kan mogelijk wel effect hebben op het vertrouwen als in de samenleving het beeld ontstaat dat er onvoldoende is gedaan om een dergelijke aanval te voorkomen. Dit is niet uit te sluiten vanwege het huidige klimaat in Nederland waarbij het handelen van de overheid onder een vergrootglas ligt.
	5.3 Sociaal-maatschappelijke impact	B	Er zal angst en onrust ontstaan en verontwaardiging, met name ook omdat het duidelijk is dat dit een aanval is. Het kan zijn dat er ook negatieve beeldvorming richting de chemische sector ontstaat (waren zij laks in het voorkomen van cyberaanvallen, waarom staan er chemische fabrieken in de buurt van woonwijken) al is de verwachting dat de maatschappelijke verontwaardiging/wantrouwen zich wellicht eerder op de overheid richt. De aanval zal niet tot polarisatie of conflicten tussen groepen leiden tenzij duidelijk is wie er achter de aanval zit en er een aanzienlijke diaspora of groep van aanhangers van deze staat bestaat. Zonder deze aspecten is de berichtgeving dat het een statelijke aanval is geweest eerder een reden voor meer saamhorigheid in Nederland.
Internationale rechtsorde en stabiliteitc	6.1 Staatssoevereiniteit, vreedzame co-existentie en vreedzame geschillenbeslechting	B	Het betreft een geweldsconflict zonder dat er sprake is van grensoverschrijding van militaire eenheden (het is een digitale aanval van een statelijke actor, maar het is niet een bewezen openlijke militaire overschrijding van de grens met troepen, hoewel dat wel zo zal worden ervaren). Het is zeer onwaarschijnlijk dat het hier een permanent lid van de VN Veiligheidsraad betreft, waardoor er geen verzwaring van de impactklasse wordt toegekend.
	6.2 Mensenrechten	C	Er is sprake van een oorlogsmisdrijf. Het is niet duidelijk of dit onderdeel is van een plan/beleid vanuit de betreffende statelijke actor waardoor het nog een hogere impact zou zijn.
	6.3 Internationaal financieel-economisch bestel	0	Niet van toepassing

Veiligheidsbelang	Criterium	Score	Toelichting
	6.4 Multilaterale instituties	B	Een dergelijke aanval door een statelijke actor kan worden gezien als het niet naleven van basisbeginselen van multinationale instituties / internationale regimes (in dit geval in elk geval de VN). Het is zeer onwaarschijnlijk dat het een normdrager/P5 betreft.
	6.5 Instabiliteit rondom Koninkrijk/EU	0	Niet van toepassing

4.3.2 Scenario collateral damage

Incidenten uit het recente verleden, met NotPetya en WannaCry als meest in het oog springende voorbeelden, laten zien dat bedrijven ook onbedoeld geraakt kunnen worden bij conflicten tussen andere (statelijke) actoren. Het gaat hierbij vaak om zogenaamde 'supply chain' incidenten, waarbij de verspreiding van de aanval plaatsvindt via een toeleverancierssketen. In dit scenario wordt een variant van een dergelijke situatie uitgewerkt, waarbij Nederland relatief hard getroffen wordt omdat de verstoring wordt veroorzaakt door malware in vrij generieke software die in veel verschillende sectoren gebruikt wordt.

Bouwstenen

In Tabel 13 is het scenario weergegeven aan de hand van de factoren en actoren. Omdat de tijd tot herstel (en dus de duur van verstoring) per organisatie verschilt (bijvoorbeeld afhankelijk van hoeveel computers opnieuw geïnstalleerd moeten worden en of er een eigen IT afdeling is), is een range van 2 dagen tot 4 weken gekozen. In de praktijk kan het in uitzonderlijke gevallen ook nog korter of langer duren, maar dit geeft een indicatie van de bandbreedte. In het scenario worden een aantal concrete sectoren en typen organisaties genoemd die getroffen worden. Deze zijn ook weergegeven in de categorie getroffenen (keteneffecten, want de oorsprong zit bij de leverancier van de software), al is het goed denkbaar dat ook organisaties uit andere categorieën getroffen worden bij dit type gebeurtenis.

Verhaallijn

Een staats-ondersteunde hackersgroep uit Iran heeft een succesvolle hack uitgevoerd op een software leverancier uit India die populaire administratiesoftware [65] verkoopt die wereldwijd gebruikt wordt door publieke en private organisaties in verschillende sectoren. Via de hack zijn de daders in staat om een malafide beveiligingsupdate voor de software beschikbaar te stellen aan de softwaregebruikers. Op het moment dat een gebruiker deze update uitvoert wordt de betreffende computer geïnfecteerd met malware. De malware stelt de aanvallers in staat om de organisatie en structuur van het netwerk in kaart te brengen.
De malware staat in verbinding met de aanvallers om verkregen informatie terug te sturen en om op basis van nieuwe opdrachten zich verder te kunnen verspreiden. Doordat de hackers een fout maakten in de code raken besturingssystemen van de betreffende computers corrupt. Hierdoor lijkt de disruptie veroorzaakt te zijn door een malafide update voor het besturingssysteem, terwijl in werkelijkheid de update van de administratiesoftware gecompromitteerd is.

Omdat veel organisaties actief beleid voeren om beveiligingsupdates snel uit te voeren verspreidt de malware zich in korte tijd snel, ook bij verschillende organisaties die actief zijn in Nederland, waaronder een aantal petrochemische bedrijven, bedrijven in de transportsector, zorginstellingen, de belastingdienst, mediabedrijven en een grote supermarktketen. Ook enkele vitale aanbieders (energiesector, financiële sector, politie) worden geraakt in hun kantoorautomatisering. Vooral bij bedrijven die afhankelijk zijn van complexe planningen leidt de verstoring in de kantoorautomatisering ook tot ernstige problemen in de operationele processen. Ondanks dat er vaak geen directe netwerkkoppeling is met de kantoorautomatisering ontstaan er problemen omdat er een functionele koppeling bestaat tussen de administratieve en operationele omgevingen. Een aantal organisaties zien zich genoodzaakt de productie- of distributiecapaciteit tijdelijk te verlagen omdat het handmatig uitvoeren van enkele geautomatiseerde processen (versturen en ontvangen van orders bijvoorbeeld) veel meer tijd in beslag neemt, maar ook omdat de oorzaak en bijwerkingen van de verstoring nog niet geduid zijn.

65 Het betreft generieke software die door bedrijven in verschillende sectoren (publiek en privaat) wordt gebruikt. Het is niet zo groot als bijvoorbeeld Microsoft of SAP, maar wel redelijk wijdverspreid.

Tabel 13 Factoren en actoren scenario collateral damage

Oorzaak	Actor	Motief	Middelen	Aard van de aantasting
Moedwillig	Statelijke actoren	(Geo-) politieke doelstelling	Malware infectie (inclusief ransomware)	Aantasting van beschikbaarheid

Tabel 13 Factoren en actoren scenario collateral damage (vervolg)

Getroffenen (direct)	Getroffenen (keteneffecten)	Doordringingsgraad	Duur
Digitale dienstverleners	Vitale aanbieders	Klein deel van de betreffende categorieën is getroffen (<10%)	2 tot 6 dagen
	Rijksoverheid		1 tot 4 weken
	Topsectoren		
	Overige organisaties (incl. gemeenten, veiligheidsregio's, MKB)		

Al snel ontstaat er brede media aandacht voor de aanval en ook de link met de beveiligingsupdate van de betreffende software wordt al na korte tijd bekend. Hierdoor wordt in veel andere organisaties het uitvoeren van updates tegengehouden. Hierdoor verspreidt de malware zich na enkele uren nauwelijks verder. De getroffen bedrijven hebben echter nog geen oplossing en zien zich gedwongen om handmatig alle getroffen computers opnieuw te installeren en configureren. Dit kan, afhankelijk van de organisatie, enkele dagen tot twee weken in beslag nemen.

Beoordeling van de impact en waarschijnlijkheid

De gevolgen van de gebeurtenissen in dit scenario zijn nog relatief beheersbaar omdat de verspreiding vrij snel stopt (dit is ook in lijn met realistische gebeurtenissen). Omdat dit type incidenten al met enige regelmaat voorkomt kan dit scenario als een 'normgevend' scenario worden gezien. Het is niet ondenkbaar dat dit type gebeurtenis nog veel ernstiger impact kan hebben, maar dan zal de waarschijnlijkheid wel aanzienlijk lager liggen.

Een belangrijke vraag bij de inschatting van de impact is de mate waarin deze gebeurtenissen een verstorend effect kunnen hebben op de continuïteit van **vitale processen**. Zoals ook in het scenario beschreven wordt, is het zeer aannemelijk dat ook vitale aanbieders getroffen worden, maar het is onzeker in hoeverre dit ook daadwerkelijk zorgt voor een verstoring van vitale processen. Veel vitale processen kunnen relatief onafhankelijk van kantoorautomatisering blijven doorgaan, al kunnen er wel ernstige problemen optreden, zeker als het herstel langer duurt (het handmatig opvangen van bepaalde activiteiten zoals logistieke planningen kan maar zeer beperkt plaatsvinden). In dit geval lijkt het in ieder geval aannemelijk dat een deel van het **betalingsverkeer** geraakt wordt, net als een deel van de **grootschalige productie/verwerking en/of opslag (petro)chemische stoffen**. Ook de **scheepvaartafwikkeling** kan mogelijk geraakt worden door de logistieke problemen in sommige sectoren.

Tabel 14 Scorekaart scenario collateral damage

Thema	Cyberdreigingen		
Dreigingscategorie	Verstoring cyber-fysieke systemen		
Scenario	Collateral damage		
Scenariotoelichting	Verstoring van kantoorautomatisering en daaraan gekoppelde proces en controle systemen (digitale sabotage). Dit ontstaat als collateral damage van een cyberaanval elders in de wereld (Staatsondersteunde hackersgroep uit Iran dat zich richt op een Indiaas softwarebedrijf)		
Waarschijnlijkheidsbeoordeling (binnen 5 jaar)			**Toelichting**
Waarschijnlijkheid:		E	Er zijn reeds voorbeelden van dergelijke incidenten met collateral damage (NotPetya enWannacry). We zijn kwetsbaar en hebben beperkte capaciteiten om er mee om te gaan. Bedrijven zijn vaak ook onvoldoende voorbereid. De impact is relatief beperkt en dat ondersteunt ook deze waarschijnlijkheid, bij veel ernstiger impact op een aantal criteria, bijvoorbeeld wanneer er meerdere vitale processen ernstig verstoord raken, wordt ook de kans dat dat allemaal tegelijkertijd optreedt lager
Beoordeling gevolgen (impact)			
Veiligheidsbelang	**Criterium**	**Score**	**Toelichting**
Territoriaal	1.1 Grondgebied	0	Niet van toepassing.
	1.2 Internationale positie	A	Iran geeft het niet toe, maar wellicht zijn er wel publieke protesten in Iran richting het Westen om woede over de manier waarop Iran (weer) wordt weg gezet als kwaad.
	1.3 Digitale ruimte	C	Er worden meerdere vitale aanbieders uit verschillende vitale processen geraakt (aanzienlijke omvang). De aanval is niet expliciet tegen hen gericht dus geen verhoging ivm motief. Wel kunnen de getroffen organisaties relatief snel maatregelen treffen om de inbreuk tegen te gaan, waardoor de impact met 1 klasse verlaagd wordt.
	1.4 Bondgenootschappelijk grondgebied	0	Niet van toepassing.
Fysiek	2.1 Doden	A	Het is niet ondenkbaar dat er dodelijke slachtoffers vallen. De aanname hierbij is wel dat de energievoorziening niet geraakt wordt. Veel andere sectoren hebben back-up mogelijkheden of kunnen met verminderde capaciteit doordraaien.
	2.2 Ernstig gewonden en chronisch zieken	A	Het is niet ondenkbaar dat er slachtoffers vallen. De aanname hierbij is wel dat de energievoorziening niet geraakt wordt. Veel andere sectoren hebben back-up mogelijkheden of kunnen met verminderde capaciteit doordraaien.
	2.3 Gebrek primaire levensbehoeften	0	Niet van toepassing, wat geraakt wordt kent alternatieven.

Veiligheidsbelang	Criterium	Score	Toelichting
Economisch	3.1 Kosten	C	Inschatting is dat de kosten van dit incident de grens van 500 miljoen zullen overschrijden, er van uitgaande dat Nederlandse bedrijven bij dit incident relatief hard geraakt worden (gebaseerd op wereldwijde schade bij vergelijkbare incidenten). De kosten betreffen voornamelijk financiële schade en hoge herstelkosten bij de getroffen grote bedrijven en het MKB. De vraag is wel of er voldoende capaciteit is voor (snel) herstel, waardoor de tijd tot herstel ook voor sommige bedrijven kan oplopen.
	3.2 Aantasting vitaliteit	0	Niet van toepassing
Ecologisch	4.1 Aantasting natuur en milieu	0	Niet van toepassing
Sociaal-politiek	5.1 Verstoring dagelijks leven	B	1 indicator (werk), tot 1 week, inschatting tussen 100.000-1 miljoen mensen.
	5.2 Aantasting democratische rechtsstaat	0	Niet van toepassing. Enige impact in functioneren van openbaar bestuur, veiligheidssysteem is denkbaar; maar het betreft niet gerichte (fysieke) belemmering, heeft geen structureel karakter en ook niet voor lange duur.
	5.3 Sociaal-maatschappelijke impact	B	Mensen gaan hamsteren, maken zich zorgen; de politiek maatschappelijke impact kan groter zijn..
Internationale rechtsorde en stabiliteit	6.1 Staatssoevereiniteit, vreedzame co-existentie en vreedzame geschillenbeslechting	A	Er is sprake van onverantwoordelijk gedrag door Iran, ze grijpen een Indiaas softwarebedrijf aan met het oogmerk dit later als machtsinstrument in te kunnen zetten. De klasse A: (beperkte schending), blokkades via infiltratie, sabotage sluit dan aan bij de aard van de acties.
	6.2 Mensenrechten	0	Niet van toepassing
	6.3 Internationaal financieel-economisch bestel	0	Niet van toepassing
	6.4 Multilaterale instituties	A	Men (in dit geval Iran) onttrekt zich aan afspraken om elkaar niet in het cyberdomein (internationaal regime) aan te grijpen.
	6.5 Instabiliteit rondom Koninkrijk/EU	0	Niet van toepassing

4.4 Beschouwing

Deze categorie laat zien dat cyberaanvallen en -incidenten een serieuze dreiging vormen voor allerlei processen in de samenleving. Cyber-fysieke systemen zijn een belangrijk onderdeel van onze digitale infrastructuur geworden en daarmee ook een mogelijk aantrekkelijk doelwit voor kwaadwillenden. De gevolgen kunnen uiteenlopen van relatief kortdurende verstoring en ontwrichting tot zeer ernstige fysieke impact met ingrijpende geopolitieke/ militaire gevolgen. De impact van de gebeurtenissen in deze twee scenario's is weliswaar relatief beperkt, maar er zijn ook situaties denkbaar waarbij de impact veel groter kan zijn (met een lagere waarschijnlijkheid). Wanneer bijvoorbeeld de energievoorziening door een dergelijke gebeurtenis ernstig verstoord wordt, of wanneer door een digitale sabotage aanval meerdere organisaties in een sector gelijktijdig worden getroffen en er op verschillende plekken een chemisch of ander soortig incident ontstaat.

De waarschijnlijkheid van de gebeurtenissen loopt sterk uiteen. Een gebeurtenis zoals in het collateral damage scenario staat beschreven is al een aantal keer voorgekomen en het is dus ook zeer waarschijnlijk dat dit type gebeurtenissen nog vaker zullen gebeuren. Hierbij hangt de omvang van de impact met name af van welke sectoren en organisaties getroffen worden. Een moedwillige sabotage aanval op een Nederlands industrieel proces is minder waarschijnlijk omdat een dergelijke actie zeer ernstige politieke of militaire gevolgen kan hebben. Het motief om tot een dergelijke actie over te gaan in Nederland is over het algemeen niet erg sterk, hoewel dit ook weer zou kunnen veranderen als de geopolitieke situatie zich wijzigt. De veiligheidsdiensten geven aan dat vitale processen (waaronder ook de ICS die binnen die processen gebruikt wordt) doelwit zijn van cyberaanvallen, tot op heden zonder een escalatie naar sabotage maar het is aannemelijk dat er wel informatie wordt vergaard of zelfs voorbereidingen worden getroffen.

5. Dreigingscategorie cybercrime

Deze risicocategorie richt zich op het fenomeen cybercrime. Door experts op het gebied van cybercrime wordt onderscheid gemaakt tussen twee verschillende fenomenen, namelijk cybercrime en cyber-enabled crime. [66] Cybercrime – de focus van deze dreigingscategorie – gaat over criminaliteit gericht op een digitaal systeem of de informatie in een systeem. Denk hierbij aan DDoS-aanvallen, ransomware of phishing. Cyber-enabled crime gaat om traditionele criminaliteit die met behulp van systemen en netwerken wordt gepleegd, denk bijvoorbeeld aan drugs- en wapenhandel of fraude. [67] Aangezien bij veel vormen van criminaliteit in toenemende mate gebruik wordt gemaakt van ICT middelen, kunnen veel vormen van criminaliteit in toenemende mate onder cyber-enabled crime worden geschaard. Zo wordt bij veel delicten binnen de georganiseerde criminaliteit ook gebruik gemaakt van ICT middelen, denk bijvoorbeeld aan drugs- en wapenhandel via online marktplaatsen, het witwassen van geld middels cryptovaluta of criminele communicatie via versleutelde chatdiensten. In deze dreigingscategorie gaan we niet in op vormen van cyber-enabled crime, maar aspecten daarvan zijn wel relevant voor bijvoorbeeld het thema ongewenste inmenging en ondermijning democratische rechtstaat, waarin ook aandacht is voor het fenomeen georganiseerde criminaliteit.

Cybercrime richt zich op zowel bedrijven als burgers en kan grote maatschappelijke impact hebben. De kosten die gepaard gaan met cybercrime groeien jaarlijks, en mede door het ontstaan van cybercrime "as-a-service" is een omvangrijke, volwassen cybercrime economie ontstaan. [68] Door de steeds verdere opkomst van state sponsored cybercrime én een enorm toename van het aantal ransomware aanvallen, waar regelmatig aandacht aan wordt besteed in de media, wordt cybercrime in toenemende mate gezien als een bedreiging van nationale veiligheid. [69] Hoewel veel individuele gevallen van cybercrime niet snel de nationale veiligheid zullen raken, aangezien de schade en kosten hiervoor over het algemeen te gering zijn, neemt de impact van het fenomeen als geheel in de samenleving steeds verder toe. Ook valt niet uit te sluiten dat er maatschappelijke ontwrichting kan ontstaan wanneer gelijktijdig meerdere organisaties in een sector of in verschillende sectoren getroffen worden en ook vitale processen kunnen doelwit zijn van cybercrime. Om deze reden is deze categorie wel binnen de analyse meegenomen.

5.1 Relevante ontwikkelingen

Cybercrimineel ecosysteem

De afgelopen jaren worden diensten en goederen die kunnen worden ingezet voor cybercrime in toenemende mate "as-a-service'" aangeboden. Denk bijvoorbeeld aan infrastructuur voor ransomware, phishing kits en DDoS aanvallen, maar ook aan gelekte accountgegevens. [70]
Er wordt vaak technische ondersteuning verleend om deze middelen in te zetten voor cyberaanvallen. Dit zorgt ervoor dat het relatief gemakkelijk is om criminele activiteiten uit te voeren. Ook betekent het dat deze activiteiten toegankelijk zijn voor een grote groep daders; men heeft geen diepgaande technische kennis nodig om een aanval uit te voeren of om betalingsgegevens van personen te bemachtigen. Het CSBN 2021 spreekt hierdoor van een cybercrimineel ecosysteem met een dienstverlenings-

66 Er zijn meerdere termen om dit onderscheid te maken, zoals 'cybercrime in enge zin' en 'cybercrime in ruime zin', of 'computer-focused crime' en 'computer-assisted crime'.
67 NCTV, Cybersecuritybeeld Nederland (CSBN) 2020 (Den Haag: 2020), https://www.ncsc.nl/documenten/publicaties/2020/juni/29/csbn-2020
68 NCTV, Cybersecuritybeeld Nederland (CSBN) 2021.
69 GFCE meeting "Trends in Cyber Crime" (22 september 2021).
70 Europol, European Union Serious and Organised Crime Threat Assessment (SOCTA) 2021. A corrupting influence: the infiltration and understanding and undermining of Europe's economy and society by organised crime (Luxembourg: Publications Office of the European Union, 2021), https://www.europol.europa.eu/publication-events/main-reports/european-union-serious-and-organised-crime-threat-assessment-socta-2021.

economie. [71] Naast dienstverleners en afnemers opereren ook autonome groepen in dit ecosysteem. Zij beschikken over veel middelen en technische kennis, en zijn hierdoor in staat om langdurige, geavanceerde aanvalscampagnes op te zetten. In sommige gevallen werken deze groepen samen met statelijke actoren. Zo bleek in 2019 dat een staatsgelieerde hackersgroep zich bezig hield met zowel spionage als financieel gemotiveerde operaties. [72]
De verwevenheid met statelijke actoren maakt het, samen met het internationale karakter van cybercrime, nog lastiger om deze groepen op te sporen en te vervolgen. [73]

Verbeterde OPSEC

De *operational security* van cybercriminelen, oftewel OPSEC, is afgelopen jaren sterk verbeterd, waardoor criminelen beter in staat zijn hun eigen identiteit te verbergen. [74]
Zo is men op de TOR browser van V2 overgegaan op V3, wat onder andere een verbetering van cryptografie inhoudt en de mogelijkheden om de identiteit van de gebruiker te achterhalen door netwerkverkeer af te vangen verhindert. Gebruikers van TOR worden eraan herinnerd om Javascript uit te schakelen en captcha's, die worden gebruikt om te controleren of er sprake is van een menselijke gebruiker, zijn verbeterd. Hierdoor kunnen deze niet meer door bots worden ingevuld. Het gebruik van cryptomunten maakt het lastig voor de politie om geldstromen te identificeren die gelinkt zijn aan criminele activiteit.

Daarnaast zijn criminelen zich steeds meer bewust van de technieken die de politie gebruikt om hun identiteit te kunnen achterhalen. De beschikbaarheid van pentesting software om te testen hoe goed hun OPSEC is, zorgt ervoor dat deze verder kan worden verbeterd. [75] Al deze maatregelen zorgen ervoor dat criminelen zich nog meer kunnen verzekeren van hun anonimiteit op het internet, waardoor ze makkelijker kunnen manoeuvreren in de digitale ruimte. De uitdaging die dit voor politie en opsporingsdiensten vormt is reeds erkend door wetmakers; in de dreigingscategorie verstoring functioneren internet is genoemd dat onder andere het toegenomen gebruik van cryptografie door criminelen heeft geleid tot discussies over het inbouwen van *master keys* in cryptografische oplossingen, waarmee overheden waar nodig versleutelde informatie zou kunnen ontcijferen.

De hoge mate van anonimiteit die de verbetering in OPSEC biedt, geldt voor het dark web, maar ook voor het *clear web*, oftewel het publiek toegankelijke Internet. In de afgelopen jaren heeft criminele activiteit op het clear web zich sterk ontwikkeld. Op platformen zoals Telegram, Discord en Wickr, of via *single vendor shops* worden onder andere drugs, wapens, gestolen gegevens, en meer recentelijk Corona herstelbewijzen en QR codes verkocht. [76] Ook voor deze platformen geldt dat het eenvoudig is om de identiteit van (ver)kopers te verbergen. *Single vendor shops* op het clear web wisselen regelmatig van hostingpartij, wat het moeilijk maakt voor de politie om te interveniëren. Door dergelijke praktijken wordt het steeds makkelijker om op het *clear web* criminele activiteiten uit te voeren.

71 NCTV, Cybersecuritybeeld Nederland (CSBN) 2021.
72 NCTV, Cybersecuritybeeld Nederland (CSBN) 2020.
73 NCTV, Cybersecuritybeeld Nederland (CSBN) 2021.
74 Europol, Internet Organised Crime Threat Assessment (IOCTA) 2020 (Luxembourg: Publications Office of the European Union, 2020), https://www.europol.europa.eu/publications-events/main-reports/internet-organised-crime-threat-assessment-iocta-2020.
75 Ibid.
76 Ibid.

Georganiseerde criminaliteit

De verbeterde OPSEC en groeiende online handels- en ontmoetingsplaatsen wijzen er op dat traditionele en cybercriminaliteit steeds verder met elkaar vervlochten raken. Criminelen weten elkaar online beter te vinden, het is makkelijk om zich te organiseren en om faciliterende diensten en goederen die online worden aangeboden te gebruiken voor criminele doeleinden. Naast cybercriminaliteit stelt dit criminelen ook in staat om makkelijker misdaden in de fysieke wereld te plegen; de beschikbaarheid van wapens en gevaarlijke stoffen, maar van ook persoonsgegevens via digitale platformen zorgt ervoor dat deze in de fysieke wereld kunnen worden misbruikt.

Ransomware

De afgelopen jaren is er veel aandacht geweest voor het gebruik van ransomware door criminelen, wat als één van de meest schadelijke trends binnen het cybercrime veld wordt gezien. De inzet van ransomware, waarbij systemen worden vergrendeld en pas worden vrijgegeven na betaling van een som losgeld, kan de operatie van bedrijven volledig platleggen. Ook de afgelopen jaren heeft ransomware veel schade veroorzaakt. Zo werd Colonial Pipeline, beheerder van de grootste oliepijplijn van de Verenigde Staten, gedwongen om de operatie tijdelijk stop te zetten, wat resulteerde in olietekorten in de hele Oostkust van de VS. [77]

Ook in Nederland kunnen vitale aanbieders worden getroffen, wat de continuïteit van vitale processen in gevaar kan brengen en een grote impact kan hebben op de maatschappij. Hoewel in Nederland tot dusver nog geen gevallen bekend zijn van vitale aanbieders die zijn geraakt, hebben ransomware aanvallen op lagere overheden plaatsgevonden, zoals de aanval op het Hof van Twente in december 2020. [78] Ook universiteiten en ziekenhuizen zijn de afgelopen jaren door ransomware getroffen. [79]

Een nieuwe ontwikkeling bij het gebruik van ransomware is dat de slachtoffers verder onder druk worden gezet om te betalen door gevoelige data te publiceren of te verkopen, of door ransomware te combineren met bijvoorbeeld DDoS aanvallen. [80] Dit maakt de impact op bedrijven of personen nog groter.

77 Turton en Mehrotra, "Colonial Pipeline Cyber Attack: Hackers Used Compromised Password".

78 Huib Modderkolk, "'Hello, need data back? Contact us fast. Hackers eisen geld van gemeente Hof van Twente," De Volkskrant (7 december 2020), https://www.volkskrant.nl/nieuws-achtergrond/hello-need-data-back-contact-us-fast-hackers-eisen-geld-van-gemeente-hof-van-twente~b6c46cff/; Brandon Vigliarolo, "Local governments continue to be the biggest target for ransomware attacks," TechRepublic (27 augustus 2020), https://www.techrepublic.com/article/local-governments-continue-to-be-the-biggest-target-for-ransomware-attacks/.

79 Joost Schellevis en Ben Meindertsma, "Zeker vijftien ziekenhuizen geïnfecteerd met ransomware," NOS Nieuws (25 juni 2017), https://nos.nl/artikel/2179941-zeker-vijftien-ziekenhuizen-geinfecteerd-met-ransomware; NOS, "Hackers Universiteit Maastricht zaten maanden in netwerk; 200.000 euro betaald," NOS Nieuws (5 februari 2020), https://nos.nl/artikel/2321732-hackers-universiteit-maastricht-zaten-maanden-in-netwerk-200-000-euro-betaald.

80 Europol, Internet Organised Crime Threat Assessment (IOCTA) 2020; NCSC Maandmonitor november 2021; GFCE meeting "Trends in Cyber Crime" (22 september 2021); KIVI webinar "Terugblik op Trends in Cybersecurity" (8 september 2021); Janus Agcaoili, Miguel Ang, Earle Earnshaw, Byron Gelera, and Nikko Tamaña, "Ransomware Double Extortion and Beyond: REvil, Clop, and Conti," Trend Micro (15 juni 2021), https://www.trendmicro.com/vinfo/us/security/news/cybercrime-and-digital-threats/ransomware-double-extortion-and-beyond-revil-clop-and-conti.

5.2 Overzicht van mogelijke actoren en factoren

Cybercrime kan op verschillende manieren tot uiting komen, er is sprake van een aantal delicten [81] en middelen [82] die gebruikt kunnen worden door uiteenlopende actoren [83] en die zich kunnen richten op verschillende soorten potentiële slachtoffers. In Tabel 15 wordt een overzicht gegeven van de actoren en factoren die worden gebruikt om tot een keuze te komen bij het ontwikkelen van het scenario. Hiermee kan worden aangegeven welke actor de dreiging veroorzaakt, welk delict wordt gepleegd en welkmiddel daarbij wordt gebruikt. Daarnaast wordt aangegeven welke van de BIV factoren wordt aangetast en welke partijen direct of indirect worden getroffen. De doordringingsgraad geeft de mate waarin de doelwitcategorie is getroffen in het scenario. Ten slotte wordt aangegeven hoe lang de verstoring en de effecten daarvan duren.

Tabel 15 Actoren en factoren dreigingscategorie cybercrime

Actor	Delict	Middel	Aard van de aantasting
Autonoom crimineel samenwerkingsverband	Diefstal	Distributed Denial of Service (DDoS)	Aantasting van beschikbaarheid
Aanbieders van 'Crime as a service' [84]	Afpersing	Misconfiguratie	Aantasting van integriteit
Individuele cybercrimineel	Fraude	Fysieke aantasting (explosie, kabel stuk, etc.)	Aantasting van betrouwbaarheid
Cybervandalen en scriptkiddies	Verstoring, vernieling en sabotage	Malware infectie (inclusief ransomware)	
		Misbruik van kwetsbaar-heden	
		Social engineering (incl. phishing)	
		....	

81 Opsomming afkomstig uit Frank Boerman, Martin Grapendaal, Fred Nieuwenhuis, Ewout Stoffers, Nationaal Dreigingsbeeld Georganiseerde Criminaliteit 2017 (Zoetermeer: Politie, 2017), https://www.politie.nl/binaries/content/assets/politie/onderwerpen/nationaal-dreigingsbeeld/2017/nationaal-dreigingsbeeld-2017.pdf.

82 Opsomming afkomstig uit NCSC, Cybercrime, van herkenning tot aangifte (Den Haag: NCSC, 2012), https://www.ncsc.nl/documenten/publicaties/2019/juli/18/handreiking-cybercrime. In de praktijk lopen de verschillende werkwijzen veelal door elkaar.

83 NCTV, Cybersecuritybeeld Nederland (CSBN) 2021.

84 Hierbij worden criminelen ingehuurd door een derde partij. De identiteit van deze partij is vaak moeilijk te achterhalen. 'Crime as a service' wordt onder andere ingezet door statelijke actoren als onderdeel van hybride operaties.

Tabel 15 Actoren en factoren dreigingscategorie cybercrime (vervolg)

Getroffenen (direct)	Getroffenen (keteneffecten)	Doordringingsgraad	Duur
Vitale aanbieders	Vitale aanbieders	Klein deel van de betreffende doelwitcategorie(ën) is getroffen (<10%)	Tot 1 dag
Rijksoverheid	Rijksoverheid	Aanzienlijk deel van de betreffende doelwitcategorie(ën) is getroffen (10-50%)	2 tot 6 dagen
Digitale dienstverleners	Digitale dienstverleners	Merendeel van de betreffende doelwitcategorie(ën) is getroffen (>50%)	1 tot 4 weken
Topsectoren	Topsectoren		1 tot 6 maanden
Kennis instellingen	Kennis instellingen		Half jaar of langer
Overige organisaties (incl. gemeenten, veiligheids-regio's, MKB)	Overige organisaties (incl. gemeenten, veiligheids-regio's, MKB)		Onherstelbaar
Burgers	Burgers		

5.3 Scenario's

Binnen de categorie cybercrime is gekozen om een scenario rondom ransomware te beoordelen, aangezien dit fenomeen door de groeiende impact op bedrijven, overheden en personen de afgelopen jaren veel aandacht heeft gekregen. In dit scenario is er voor bewust voor te kozen om niet een vitaal proces als doelwit te kiezen, aangezien een dergelijk scenario in de themarapportage bedreiging vitale infrastructuur wordt behandeld (scenario ransomware aanval telecomprovider). In aanvulling op dat scenario is er hier gekozen voor een ransomware aanval waarbij een groot aantal organisaties (ziekenhuizen) in dezelfde sector gelijktijdig geraakt worden omdat het een supply chain aanval betreft.

5.3.1 Scenario ransomware aanval ziekenhuizen

In het scenario ransomware aanval ziekenhuizen wordt een aanval beschreven waarbij een groot aantal Nederlandse ziekenhuizen via een leverancier worden getroffen door ransomware. Zoals vele andere sectoren, zijn ook in de zorgsector gevallen bekend van organisaties die zijn geraakt door ransomware. Zo werden in 2020 meer dan 600 ziekenhuizen en klinieken in de Verenigde Staten geraakt door ransomware. [85] Ook in Nederland zijn ziekenhuizen slachtoffer geworden, zo werd in 2017 melding gemaakt een aantal ziekenhuizen die door ransomware werd getroffen. [86] In sommige gevallen wordt één organisatie geraakt, in andere gevallen worden meerdere organisaties getroffen, zoals het geval was bij het WannaCry virus in 2017, waarbij naar schatting 80 ziekenhuizen in het Verenigd Koninkrijk werden getroffen. [87]

Verhaallijn

Een hackersgroepering [88] slaagt erin een grote Nederlandse aanbieder van het Elektronisch patiëntendossier (EPD) te compromitteren via social engineering. Middels de verkregen toegang wordt de aanbieder besmet met ransomware, waardoor de systemen en bestanden van het bedrijf worden versleuteld. [89] omdat dit een van de grote leveranciers van EPD is, worden veertig ziekenhuisorganisaties hierdoor geraakt. Zij ondervinden onmiddellijk proble men door de aanval omdat zij geen toegang meer hebben tot het EPD, waardoor zij niet kunnen beschikken over onder andere patiëntgegevens en uitschrijfsystemen voor medicijnrecepten niet meer functioneren.

De aanval komt tijdens de Coronapandemie, waarin de zorg al flink onder druk staat. Ten gevolge van de aanval zullen sommige ziekenhuizen geen nieuwe patiënten opnemen, hun SEH sluiten of moeten besluiten om operaties en MRI scans uit te stellen. Daarnaast wordt een ad-hoc papieren administratie van patiënt- en behandelgegevens opgezet. Men heeft geen informatie meer over reeds toegediende medicatie en behandelmethoden, waardoor artsen af moeten gaan op hun eigen inschattingen en eventueel de informatie die de patiënt kan geven.

Tabel 16 Factoren en actoren scenario ransomware aanval ziekenhuizen

Actor	Delict	Middel	Aard van de aantasting	Getroffenen (direct)	Doordringingsgraad	Duur
Autonoom crimineel samenwerkings-verband	Verstoring, vernieling en sabotage	Malware infectie (inclusief ransomware)	Aantasting van beschikbaarheid	Overige organisaties (incl. gemeenten, veiligheidsregio's, MKB)	Klein deel van de betreffende doelwitcategorie(ën) is getroffen (<10%)	1 tot 4 weken
		Social engineering (incl. phishing)				

85 Paul Bischoff, "Ransomware attacks on US healthcare organizations cost $20.8bn in 2020," Comparitech (10 maart 2021), https://www.comparitech.com/blog/information-security/ransomware-attacks-hospitals-data/#How_much_did_these_ransomware_attacks_cost_healthcare_organizations_in_2020.

86 Schellevis en Meindertsma, "Zeker vijftien ziekenhuizen geïnfecteerd met ransomware".

87 Heather Landi, "Report: 40% of healthcare organizations hit by WannaCry in past 6 months," Fierce Healthcare (29 mei 2019), https://www.fiercehealthcare.com/tech/lingering-impacts-from-wannacry-40-healthcare-organizations-suffered-from-attack-past-6-months; Thomas B. Slayton, "Ransomware: The Virus Attacking the Healthcare Industry," Journal of Legal Medicine 38, no. 2 (April 2018): 287-311, https://doi.org/10.1080/01947648.2018.1473186.

88 Bijvoorbeeld een groepering als UNC 1878/Wizard Spider: Lily Hay Newman, "Ransomware Hits Dozens of Hospitals in an Unprecedented Wave," Wired (29 oktober 2020), https://www.wired.com/story/ransomware-hospitals-ryuk-trickbot/.

89 Bijvoorbeeld ransomware Ryuk: "Z-CERT waarschuwt voor mogelijke opmars ransomware," ICT&health (5 november 2020), https://www.icthealth.nl/nieuws/z-cert-waarschuwt-voor-mogelijke-opmars-ransomware/.

In de eerste uren na het uitvallen van het EPD heerst er grote verwarring en onduidelijkheid. Vanwege het grote aantal ziekenhuizen dat problemen ondervindt kunnen in veel regio's geen patiënten worden overgebracht naar omliggende ziekenhuizen. Binnen ziekenhuizen en ambulancediensten is geen goed overzicht over welke organisaties precies zijn getroffen en waar bedden beschikbaar zijn voor nieuwe patiënten. Ten gevolge hiervan duurt het langer om patiënten de hulp te bieden die zij nodig hebben, aangezien ambulancepersoneel eerst moet achterhalen welk ziekenhuis bedden beschikbaar heeft en soms langere afstanden moet afleggen om het ziekenhuis te bereiken. Daarnaast worden op sociale media al snel berichten verspreid over ziekenhuizen die niet of juist wel beschikbaar zijn, wat de verwarring vergroot. Als de schaal van de aanval duidelijk wordt, wordt de nationale crisisstructuur opgeschaald om de verstoring op te vangen. Er worden veldhospitalen opgezet waar patiënten terecht kunnen.

Ondertussen wordt er hard gewerkt om de aanbieder van het EPD weer online te krijgen en zoekt men naar alternatieven om de ziekenhuizen weer operationeel te krijgen. Sommige ziekenhuizen lukt het in 48 uur middels een back-ups om weer toegang tot de gegevens in het EPD te verkrijgen, voor anderen duurt het een aantal dagen tot een week om weer toegang te krijgen tot de informatie via back-ups of andere geïmproviseerde oplossingen.

De aanbieder van het EPD slaagt er na drie weken uiteindelijk in om de servers waar het EPD op draait weer functioneel te krijgen. Het duurt echter nog langer voordat alles weer naar behoren werkt en de dienstverlening volledig is hersteld.

Beoordeling impact en waarschijnlijkheid

Hoewel ransomware aan de orde van de dag is, wordt de waarschijnlijkheid van dit scenario met een B-score beoordeeld. De reden hiervoor is dat het onwaarschijnlijk wordt geacht dat er een grote hoeveelheid ziekenhuizen op deze manier tegelijkertijd wordt getroffen door ransomware. Hoewel het wel realistisch is dat meerdere organisaties verspreid over een aantal sectoren door één aanval worden getroffen, zoals bij WannaCry het geval was, wordt het minder voorstelbaar geacht dat een dergelijk grote hoeveelheid ziekenhuizen gericht wordt aangevallen door cybercriminelen.

Over het algemeen is de impact van de in het scenario beschreven gebeurtenissen relatief beperkt. Er ontstaat wel veel chaos en problemen in de acute ziekenhuiszorg, maar de duur hiervan is beperkt omdat er snel een crisisorganisatie kan worden opgetuigd. De IT problemen houden wel langer aan, maar de maatschappelijke ontwrichting is relatief van korte duur.

Tabel 17 Scorekaart scenario ransomware aanval ziekenhuizen

Thema	**Cyberdreigingen**	
Dreigingscategorie	Cybercrime	
Scenario	Ransomware aanval ziekenhuizen	
Scenariotoelichting	De EPD systemen van 40 ziekenhuisorganisaties worden versleuteld door ransomware dat via een hack op een grote Nederlandse aanbieder van EPD systemen is verspreid. Met name de eerste uren na het uitvallen van de EPD systemen levert dit problemen op in die ziekenhuiszorg. Na ongeveer 48 uur tot een week krijgen de meeste ziekenhuisorganisaties via een back-up of andere oplossingen weer toegang tot de gegevens in het EPD.	
Waarschijnlijkheidsbeoordeling (binnen 5 jaar)		**Toelichting**
Waarschijnlijkheid:	B	Ransomware aanvallen komen vaak voor en daarom zijn de gebeurtenissen (enigszins) voorstelbaar. De waarschijnlijkheid dat individuele ziekenhuizen getroffen worden is echter vele male groter dan een ransomware aanval via een leverancier waarbij 40 ziekenhuisorganisaties tegelijk (gericht) getroffen worden. Er zijn wel situaties waarbij vele organisaties door ransomware getroffen worden, maar dat is dan verspreid over meerdere sectoren (collateral damage). De vraag is wat het belang is van een hackersgroep om deze toch wel ingewikkelde ransomware aanval uit te voeren (gericht op afpersing van de leverancier of ook de ziekenhuizen?). Maar het valt niet uit te sluiten dat zoiets zou kunnen gebeuren (er zijn geen concrete aanwijzingen).
Beoordeling gevolgen (impact)		

Veiligheidsbelang	Criterium	Score	Toelichting
Territoriaal	1.1 Grondgebied	0	Niet van toepassing
	1.2 Internationale positie	0	Niet van toepassing. Er zouden eventueel problemen kunnen ontstaan in samenwerking (onderzoeken etc.) met buitenlandse partijen, maar dit zal naar verwachting niet leiden tot de indicatoren genoemd in dit criterium.
	1.3 Digitale ruimte	B	EPD leveranciers en ziekenhuizen zijn 'overige' organisaties. De helft van de ziekenhuizen hebben te maken met een schending (want er zit ransomware in hun systeem), dat is aanzienlijk (+1). De aanval is moedwillig, maar er is geen aanwijzing dat er een ideologisch of politiek motief achter zit, dus geen ophoging. Geen correctie voor beheersingsmaatregelen.
	1.4 Bondgenootschappelijk grondgebied	0	Niet van toepassing
Fysiek	2.1 Doden	B	De eerste uren ontstaat er een logistiek infarct, ziekenhuizen zullen patiënten willen verplaatsen en/of kunnen geen nieuwe patiënten ontvangen. Ambulances die moeten uitwijken en in verkeer vast komen te zitten. Met name in die eerste uren kunnen er situaties zijn waarin mensen te laat geholpen kunnen worden of ergens terecht kunnen, waardoor mensen kunnen overlijden.
	2.2 Ernstig gewonden en chronisch zieken	C	Door de logistieke problemen in de eerste fase kunnen er mensen zijn die niet tijdig geholpen kunnen worden. Ook in de weken erna zullen ziekenhuizen bepaalde afspraken moeten uitstellen. Hierdoor is de verwachting dat er gevallen zullen zijn van mensen waarbij de behandeling laat plaatsvindt waardoor chronische aandoeningen of ernstiger gevolgen ontstaan dan zonder deze gebeurtenissen.
	2.3 Gebrek primaire levensbehoeften	B	Het gebrek aan/verstoorde acute gezondheidszorg in een groot deel van NL zal vermoedelijk een grote groep mensen treffen. Er zal een crisisorganisatie worden opgetuigd vanuit de overheid, maar dat kan wel enige tijd in beslag nemen.

Veiligheidsbelang	Criterium	Score	Toelichting
Economisch	3.1 Kosten	B	De kosten betreffen met name herstelkosten van de EPD systemen bij al deze organisaties, bestrijdingskosten crisissituatie. De kosten van herstel na een ransomware aanval variëren. Een gemiddelde organisatie is c.a. 2,3 miljoen dollar kwijt voor herstel en kleinere organisaties (inclusief zorgorganisaties) zijn gemiddeld 1,8 miljoen kwijt. Dit is niet allemaal directe schade want hierin wordt ook het loon van ICTers die hieraan werken meegeteld. Maar dat het met 40 ziekenhuisorganisaties én de crisis-bestrijding oploopt tot >50 miljoen is niet onrealistisch. Het zal niet de grens van 500 miljoen overschrijden.
	3.2 Aantasting vitaliteit	0	Niet van toepassing
Ecologisch	4.1 Aantasting natuur en milieu	0	Niet van toepassing
Sociaal-politiek	5.1 Verstoring dagelijks leven	B	1 indicator, gemiddeld. Maatschappelijke voorzieningen: er zal spraken zijn van uitgestelde zorg gedurende een aantal weken voor <100.000 mensen.
	5.2 Aantasting democratische rechtsstaat	A	Twee indicatoren beperkt: Verlies vertrouwen in openbaar bestuur en daaraan verbonden ambtenaren, én politieke vertegenwoordiging. Effect op vertrouwen in politiek en overheid is versterkt omdat de verhoudingen al op scherp staan (o.a. coronapandemie). Samenleving is verontwaardigd dat de overheid dergelijke cyberaanvallen niet kan afweren en de zorgsector beter moet beschermen.
	5.3 Sociaal-maatschappelijke impact	B	Deze gebeurtenissen zullen tot brede maatschappelijke onrust en woede leiden, zeker wanneer er ook slachtoffers vallen én omdat er mogelijk gevoelige gezondheidsinformatie op straat komt te liggen. Ook omdat veel mensen zich niet bewust waren van de hoeveelheid data die in dit soort systemen is opgeslagen. Dit leidt tot negatieve beeldvorming en verlies van vertrouwen in zorgsector door schending van privacy. Dit grijpt in op bestaande spanningen tussen groepen irt corona en gezondheid (als gezondheidsgegevens op straat komen te liggen kan dat ook gebruikt worden om te discrimineren) en kan daarmee polarisatie doen toenemen.
Internationale rechtsorde en stabiliteit	6.1 Staatssoevereiniteit, vreedzame co-existentie en vreedzame geschillenbeslechting	0	Niet van toepassing
	6.2 Mensenrechten	0	Niet van toepassing
	6.3 Internationaal financieel-economisch bestel	0	Niet van toepassing
	6.4 Multilaterale instituties	0	Niet van toepassing
	6.5 Instabiliteit rondom Koninkrijk/EU	0	Niet van toepassing

5.4 Beschouwing

Cybercrime is een groeiend fenomeen en de verstoringen die door actoren in dit criminele ecosysteem teweeg worden gebracht zijn veelvoorkomend en kunnen een omvangrijke impact kunnen hebben. Vooral ransomware aanvallen kunnen grote problemen opleveren voor bedrijven en overheden en daarmee ook zorgen voor maatschappelijke ontwrichting. Tegelijkertijd lijkt de beoordeling van het scenario in deze dreigingscategorie het beeld te bevestigen dat een enkele ransomware aanval (zelfs als de aanval een groot aantal ziekenhuizen tegelijk treft) een relatief beperkte impact heeft op de nationale veiligheid, tenzij hierdoor een vitaal proces verstoord wordt waarbij de cascade effecten in de samenleving groot zijn. De schade die cybercriminaliteit veroorzaakt wordt dus voornamelijk bereikt door de cumulatie van aanvallen. Daarbij zijn de opkomst van *state sponsored* cybercrime en de toenemende verwevenheid tussen cybercriminaliteit en traditionele criminaliteit trends die erop wijzen dat de mogelijke impact van cybercriminaliteit als geheel de komende jaren nog verder toe zal nemen.

6. Sluimerende dreigingen

Voor het thema cyberdreigingen zijn technologische ontwikkelingen op het gebied van onder andere Artificiële intelligentie (AI) en Quantum relevant omdat de verwachting is dat ze de aard van en omvang van dreigingen binnen dit thema op termijn sterk kunnen veranderen. Twee specifieke ontwikkelingen lichtten we hier wat nader toe:

1. AI-gedreven cyberaanvallen
2. Kwetsbare cryptografie in het quantum tijdperk

AI-gedreven cyberaanvallen

Artificiële intelligentie kan op verschillende manieren toegepast als hulpmiddel bij cyberaanvallen en dit wordt dan ook gezien als een opkomende dreiging. Zo kan AI gebruikt worden om automatisch interessante targets te detecteren (bijvoorbeeld door automatische verwerking van openbare gegevens) of om automatisch kwetsbaarheden in systemen te voorspelen door patroonherkenning in gegevens van apparaten en netwerken van een gebruiker. Om vervolgens toegang te krijgen kan AI gebruikt worden om wachtwoorden te raden (bijvoorbeeld op basis van grote hoeveelheden data van gelekte wachtwoorden). Ook kunnen AI technieken ingezet worden om detectiesystemen te ontwijken, kunnen aanvallen gepersonaliseerd worden door automatische gedragsanalyse en kan malware intelligenter worden doordat het zelflerende eigenschappen krijgt waarmee het zelfstandig nieuwe kwetsbaarheden kan vinden. [90]

Hoewel een deel van deze toepassingen van AI al in de praktijk voorkomen, is het beeld dat dit op dit moment nog op een relatief beperkte schaal en voor relatief kleine sub-taken van een cyberaanval gebeurt. De verwachting is dat dit de komende jaren flink toe zal nemen door de razendsnelle ontwikkelingen op het gebied van AI en het feit dat veel informatie over deze ontwikkelingen eenvoudig openbaar online te vinden is. In principe zijn alle bouwblokken beschikbaar om in de nabije toekomst geavanceerde zelflerende en zelf-aanvallende malware te ontwikkelen. [91]

In 2018 hebben onderzoekers van IBM een nieuw type malware ontwikkeld (DeepLocker) om beter te begrijpen hoe specifieke AI modellen gecombineerd zouden kunnen worden met bestaande malware technieken. Op basis van *deep learning* technieken hebben zij laten zien dat het mogelijk is om AI-gedreven malware te ontwikkelen die niet te detecteren is, omdat het zich verborgen kan houden tot het moment dat het een specifiek doelwit bereikt heeft en dan direct in de aanval gaat. [92] Dit type malware is tot op heden nog niet buiten het onderzoekslab gesignaleerd, maar geeft wel aan dat de stap naar geavanceerde AI-gebaseerde cyberaanvallen niet ver weg lijkt te zijn.

[90] Blessing Guembe, Ambrose Azeta, Sanjay Misra, Victor Chukwudi Osamor, Luis Fernandez-Sanz en Vera Pospelova, "The Emerging Threat of Ai-driven Cyber Attacks: A Review," Applied Artificial Intelligence (2022): 1-34, https://doi.org/10.1080/08839514.2022.2037254.

[91] Guembe et al., "The Emerging Threat of Ai-driven Cyber Attacks: A Review"; Marc Ph. Stoecklin, Jiyong Jang , Dhilung Kirat, "DeepLocker: How AI Can Power a Stealthy New Breed of Malware," SecurityIntelligence (8 augustus 2018), https://securityintelligence.com/deeplocker-how-ai-can-power-a-stealthy-new-breed-of-malware/; William Dixon, Nicole Eagan, "3 ways AI will change the nature of cyber attacks," World Economic Forum (19 juni 2019), https://www.weforum.org/agenda/2019/06/ai-is-powering-a-new-generation-of-cyberattack-its-also-our-best-defence/.

[92] Stoecklin et al., "DeepLocker: How AI Can Power a Stealthy New Breed of Malware".

De inzet van AI bij cyberaanvallen heeft in algemene zin op drie manieren belangrijke implicaties voor cyberdreigingen: [93]

- Aanvallen worden steeds meer tailormade. Door steeds **nauwkeurigere nabootsing** van echte, vertrouwde gebruikers kan spam steeds overtuigender worden en gepersonaliseerd naar het beoogde slachtoffer.
- Doordat **aanvallen steeds beter vermomd worden**, kan malware lange tijd onopgemerkt geïnstalleerd zijn op een apparaat en zich verspreiden naar andere apparaten en netwerken. Daarbij kan AI malware ook snel grote hoeveelheden data analyseren om te identificeren wat waardevol is en wat niet.
- Steeds **snellere aanvallen met effectievere consequenties** zullen het moeilijker maken om aanvallen te detecteren en af te wenden. Aanvallers hebben minder mankracht nodig, terwijl bestaande beveiligingsmechanismen steeds minder weerstand kunnen bieden.

De consequenties van deze opkomende AI-gedreven cyberaanvallen kunnen potentieel zeer destructief zijn. AI-gedreven aanvallen zullen gericht en op maat gemaakt zijn en snel kunnen leren van een toepassing in een nieuwe context, met de potentie voor enorme schaalbaarheid. Daarbij zullen de aanvallen effectiever zijn dan handmatige aanvallen, met weinig tot geen noodzaak meer van inzet van menselijke capaciteit. Vertrouwelijkheid en integriteit van data zullen niet meer vanzelfsprekend zijn, en zeer effectieve en sluipende aanvallen kunnen organisaties, en daarmee ook maatschappelijke processen zwaar ontregelen. Ook het vertrouwen van werknemers en burgers in instanties, organisaties en overheden zou hierdoor af kunnen nemen. [94] Door deze ontwikkelingen zal het beveiligen van systemen met de huidige middelen een verloren race zijn, omdat het benodigde menselijk werk sterk toeneemt terwijl de hoeveelheid en de snelheid van aanvallen niet bij te houden is. Cybersecurity zal dus ook een fundamentele verandering moeten ondergaan, wellicht ook met meer inzet van AI in beveiliging- en verdedigingsmethoden. [95]

Kwetsbare cryptografie in het quantum tijdperk

Quantum technologie wordt gezien als een veelbelovende technologie met potentieel sterk disruptieve toepassingen in veel verschillende sectoren. Niet voor niets wordt er wereldwijd enorm in deze technologie geïnvesteerd. Quantum is een groot technologiegebied en daarbinnen zijn veel verschillende technologieën te identificeren, waaronder *quantum computation, quantum communication en quantum sensing*. [96] De verschillende technologieën bevinden zich in verschillende stadia van ontwikkeling en voor veel toepassingen geldt dat deze nu nog een laag technology readiness level kennen, al zijn er ook al enkele real-life toepassingen van quantum technologie beschikbaar.

Voor het thema cyberdreigingen zijn met name de ontwikkelingen op het gebied van quantum computing relevant. De enorme rekenkracht die quantum computers met zich mee zullen brengen zullen het digitale domein ingrijpend veranderen. Het is de verwachting dat het nog wel zo'n 15 jaar zal duren voordat de eerste volwaardige quantum computers operationeel zullen zijn, maar experts krijgen wel een steeds beter beeld bij de gevolgen van deze doorbraak technologie.

Hoewel het nog grotendeels onduidelijk is hoe het quantum tijdperk er uit gaat zien en wat dit betekent voor het digitale landschap zijn experts het er over eens dat het grote veranderingen teweeg zal brengen. Een van de meest concrete en kritieke dreigingen die wordt verwacht is dat quantum technologie huidige cryptografische protocollen zal breken. [97] Shor's algoritme [98] (een quantum algoritme) zal er voor zorgen dat de huidige state-of-the-art asymmetrische algoritmen niet meer voldoen voor versleuteling van gegevens. [99] Deze vorm van cryptografie vormt niet alleen de basis van de *Public Key Infrastructure* wat door veel (overheids-) diensten gebruikt wordt voor veilige, digitale authenticatie, maar het wordt ook in heel veel Internet Protocollen gebruikt, zoals bijvoorbeeld in DNSSEC. [100] Cryptografie wordt steeds belangrijker voor het

93 Dixon, Eagan, "3 ways AI will change the nature of cyber attacks".
94 Guembe et al., "The Emerging Threat of Ai-driven Cyber Attacks: A Review".
95 Cong Truong Thanh, Ivan Zelinka, "A survey on Artificial Intelligence in Malware as Next-Generation Threats," Mendel 25, no. 2 (2019): 27-34, https://doi.org/10.13164/mendel.2019.2.027; Guembe et al., "The Emerging Threat of Ai-driven Cyber Attacks: A Review".
96 Carolina van Weerd, Deborah Lassche, "National Security Implications of Quantum Technology and Biotechnology," Strategic Alert HCSS & TNO (oktober 2021), https://publications.tno.nl/publication/34638911/49Bqnv/weerd-2021-national.pdf.
97 Müller et al. "Retrofitting post-quantum cryptography in Internet protocols: A case study of DNSSEC"; Van Weerd, Lassche, "National Security Implications of Quantum Technology and Biotechnology".
98 Peter W. Shor, "Polynomial Time Algorithms for Discrete Logarithms and Factoring on a Quantum Computer," SIAM J.Sci.Statist.Comput. 26 (1997): 1-28, https://doi.org/10.48550/arXiv.quant-ph/9508027.
99 Van Weerd, Lassche, "National Security Implications of Quantum Technology and Biotechnology".
100 Müller et al. "Retrofitting post-quantum cryptography in Internet protocols: A case study of DNSSEC".

veilig functioneren van digitale systemen en diensten en daarom is de zorg over de veiligheid van cryptografische toepassingen in het licht van de quantum technologie ontwikkelingen groot en urgent.

Vanwege de verwachte problemen wordt nu al veel onderzoek gedaan naar vormen van cryptografie die bestand zijn tegen de rekenkracht van quantum computers. In dit kader wordt vaak gesproken over 'post-quantum-cryptografie' maar ook termen als 'quantum proof' of 'quantum resistant' of 'quantum safe' cryptography worden gebruikt [101] om nieuwe vormen van cryptografische toepassingen aan te duiden die nodig zullen zijn in een quantum tijdperk. Dit type onderzoek is een belangrijke stap in het voorbereid zijn op het quantum tijdperk, maar de implementatie van dergelijke oplossingen zal ook nog heel veel vragen en dat baart experts ook zorgen.
Op dit moment zijn er nog geen afspraken over een nieuwe standaard, maar om een voorbeeld te geven: één van de oplossingen voor het versterken van cryptografie is het toepassen van langere sleutels (met meer karakters) en hoewel dat relatief eenvoudig klinkt is de praktische implicatie enorm. Veel van de huidige (Internet) technologie maakt gebruik van sleutels met een heel specifieke lengte, dus het verlengen van sleutels is niet iets dat heel eenvoudig is. [102] De ervaring leert bovendien dat de uptake van belangrijke maatregelen vaak moeizaam gaat en veel tijd kost. Dit is niet iets dat een organisatie of sector van de ene op de andere dag kan invoeren, er zijn serieuze aanpassingen en updates (zowel software- als hardware-matig) nodig. Experts schatten in dat grote organisaties die veel digitale infrastructuur en legacy systemen hebben (waaronder bijvoorbeeld banken, telecom providers en andere vitale aanbieders) al gauw tien jaar nodig zullen hebben om volledig 'quantum resistant' te worden. [103]
Er zal dus hoe dan ook een lange transitieperiode bestaan waarin sommige systemen al quantum proof zijn en andere nog niet. Los van de technische en praktische uitdagingen van het upgraden van systemen om quantum proof te worden, zal ook de (politieke) discussie over standaarden en de manier waarop cryptografie ingezet wordt deze stappen mogelijk verder compliceren.

Voor de nationale veiligheid betekenen deze ontwikkelingen dat er mogelijk een sterke toename zal ontstaan van kwetsbare systemen, waarbij gevoelige informatie niet goed beveiligd meer is. Dataverkeer dat is versleuteld met 'oude cryptografie' (huidige cryptografie dus) dat door kwaadwillenden wordt onderschept (of in het verleden al eerder is onderschept) kan dan massaal ontcijferd worden waardoor die informatie misbruikt worden voor strategische (politieke of economische) doeleinden of operationele inzet (bijvoorbeeld informatie over kwetsbaarheden om allerlei verschillende typen aanvallen uit te voeren, of persoonlijke informatie die ingezet kan worden bij gerichte social engineering). Met andere woorden, de impact en waarschijnlijkheid van spionage-dreigingen (zie thema ongewenste inmenging en ondermijning democratische rechtstaat) en andere digitale aanvallen neemt dan toe. Het is dus zaak om hier nu al op te anticiperen, maar zelfs dan zal er naar verwachting een periode ontstaan waarin sommige systemen nog niet voldoende beschermd zijn volgens de nieuwste standaarden.

Het vertrouwen in de samenleving met betrekking tot digitale systemen en daarmee indirect ook het vertrouwen in de overheid en instanties kan verder onder druk komen te staan omdat er meer situaties zullen zijn waarbij gevoelige informatie niet voldoende beschermd blijkt.

Naast de specifieke problemen die te maken hebben met de kwetsbaarheid van cryptografie in het quantum tijdperk kunnen quantum computing ontwikkelingen ook op uiteenlopende andere manieren de nationale veiligheid raken. De dreiging van de eerder beschreven AI-gedreven cyberaanvallen zal bijvoorbeeld alleen nog maar toenemen wanneer dit gecombineerd wordt met de enorme rekenkracht (en snelheid) van quantum computers.

[101] Müller et al. "Retrofitting post-quantum cryptography in Internet protocols: A case study of DNSSEC"; Quantum vision team, "Quantum Internet: The internet's next big step," issuu (3 juni 2019), https://issuu.com/ tudelft-mediasolutions/docs/quantum_magazine_june_2019.
[102] Müller et al. "Retrofitting post-quantum cryptography in Internet protocols: A case study of DNSSEC".
[103] Quantum vision team, "Quantum Internet | The internet's next big step".

7. Slotbeschouwing

Binnen het thema cyberdreigingen zijn voor vijf scenario's de gevolgen en waarschijnlijkheid in kaart gebracht. Daarnaast zijn er enkele scenario's uit andere thema's die nauwe raakvlakken met het thema cyberdreigingen kennen, zoals de ransomware aanval op een telecom provider (thema bedreiging vitale infrastructuur) en het scenario cyberspionage overheid (thema ongewenste inmenging en beïnvloeding democratische rechtstaat). In Figuur 1 worden deze scenario's in vergelijkend perspectief weergegeven.

Figuur 1 Risicodiagram thema cyberdreigingen

	Zeer onwaarschijnlijk	Onwaarschijnlijk	Enigzins waarschijnlijk	Waarschijnlijk	Zeer waarschijnlijk
Catastrofaal					
Zeer ernstig				• Aanval Cloud Service Provider	
Ernstig	• Ransomeware telecom (uit thema bedreiging vitale Infrastructuur)				
Aanzienlijk		• Cyber ICS - chemische sector • Ransomeware zorgsector		• Cyberspionage overheid (uit thema ongewenste inmenging en beinvloeding democratische rechtsstaat) • Misconfiguratie grote Internetdienstverlener	• Collateral damage
Beperkt					

Het valt op dat de waarschijnlijkheid van de scenario's sterk uiteenloopt en dat de impact over het algemeen relatief beperkt blijft. Hierbij is het belangrijk om te benadrukken dat die impactbeoordeling beïnvloed wordt doordat het in veel gevallen erg moeilijk te voorspellen is wat de gevolgen zijn van verstoringen van digitale systemen, netwerken en diensten. Zoals ook al in de ANV Horizonscan Nationale Veiligheid 2020 werd geconstateerd zorgt de vernetting en digitalisering van de samenleving er voor dat "we niet goed kunnen overzien wat de impact van een digitale verstoringen is. In alle sectoren van de samenleving worden databronnen en informatiesystemen aan elkaar gekoppeld, maar vaak met onvoldoende inzicht in cascade-effecten bij uitval of nieuwe aanvalsroutes die daarmee gecreëerd worden". [104] Daar komt nog bij dat de digitale ruimte (het samenspel van IT netwerken en informatiesystemen) continu in beweging is en dat zorgt ook weer voor nieuwe, onverwachte afhankelijkheidsrelaties en effecten. De 'sluimerende dreigingen' die kunnen voortkomen uit technologische ontwikkelingen zoals AI (geavanceerde AI gebaseerde cyberaanvallen) en Quantum (kwetsbare cryptografie, waardoor protocollen en gevoelige gegevens niet meer veilig zijn én meer rekenkracht voor kwaadwillenden om geautomatiseerde aanvallen uit te voeren) laten zien dat het ook niet te verwachten is dat deze dynamiek in de toekomst zal verminderen.

Een andere oorzaak voor de relatief lage impact lijkt te zijn dat de maatschappelijke impact van de verstoringen in veel gevallen een beperkte duur kent. Door het belang van digitale systemen is er ook een (commerciële) drive bij aanbieders om problemen snel te verhelpen. In andere gevallen kunnen de maatschappelijke gevolgen na verloop van tijd opgevangen worden met alternatieven of back-up systemen terwijl de daadwerkelijke herstelwerkzaamheden nog doorgaan. Tenslotte zorgt de decentrale architectuur van het internet en internetdiensten ervoor dat veel verstoringen beperkt blijven tot een specifieke groep gebruikers of diensten. Die kunnen weliswaar wijdverspreid zijn (wereldwijd), maar de effecten zijn relatief geconcentreerd.

De impact die ontstaat vanuit cyberdreigingen is divers en verspreid over alle veiligheidsbelangen en impactcriteria. Dit is ook logisch want binnen dit thema worden ook zeer uiteenlopende typen dreigingen geadresseerd waardoor ook verschillende veiligheidsbelangen worden bedreigd. Door deze breedte van het thema en de dreigings-categorieën is het moeilijk om generaliserende conclusies te trekken over de omvang en aard van de impact van de onderliggende fenomenen in relatie tot specifieke veiligheidsbelangen of criteria.

Vanuit de in deze rapportage beschreven ontwikkelingen en de gesprekken met experts rondom de scenario's wordt opnieuw bevestigd dat de digitalisering van de samenleving (en economie) niet alleen zorgt voor nieuwe mogelijkheden én kwetsbaarheden, maar dat het ook steeds meer een onderwerp van strategisch, (geo)politiek belang is.
De dominante rol van grote techbedrijven en de manier waarop staten zich op uiteenlopende manieren mani-festeren in het digitale domein zorgen ervoor dat er spanningsvelden ontstaan tussen verschillende belangen en perspectieven op de digitale ruimte, bijvoorbeeld als het gaat om het streven naar digitale soevereiniteit of autonomie van landen en het effect daarvan op de technische ontwikkelingen/innovaties. Ook zijn er ontwikkelingen die de governance en waarden van het Internet en de digitale ruimte onder druk zetten, waardoor op termijn onze Nederlandse belangen van een open en digitale economie in het geding kunnen komen.

[104] ANV, Horizonscan Nationale Veiligheid 2020 (Bilthoven: RIVM, 2020), https://www.rivm.nl/sites/default/files/2020-11/Horizonscan%20Nationale%20Veiligheid%202020.pdf.

Bronnenlijst

Agcaoili, Janus; Ang, Miguel; Earnshaw, Earle; Gelera, Byron; Tamaña, Nikko. "Ransomware Double Extortion and Beyond: REvil, Clop, and Conti." Trend Micro (15 juni 2021), *https://www.trendmicro.com/vinfo/us/security/news/cybercrime-and-digital-threats/ransomware-double-extortion-and-beyond-revil-clop-and-conti*.

ANV. *Horizonscan Nationale Veiligheid 2020. Bilthoven: RIVM*, 2020.

ANV. *Leidra ad Risicobeoordeling Rijksbrede Risicoanalyse Nationale Veiligheid*. Bilthoven, RIVM: 2022. *https://www.rivm.nl/onderwerpen/nationale-veiligheid.*

Bischoff, Paul. "Ransomware attacks on US healthcare organizations cost $20.8bn in 2020." Comparitech (10 maart 2021). *https://www.comparitech.com/blog/information-security/ransomware-attacks-hospitals-data/#How_much_did_these_ransomware_attacks_cost_healthcare_organizations_in_2020*

Boerman, Frank; Grapendaal, Martin; Nieuwenhuis, Fred; Stoffers, Ewout. N*ationaal Dreigingsbeeld Georganiseerde Criminaliteit 2017* (Zoetermeer: Politie, 2017). *https://www.politie.nl/binaries/content/assets/politie/onderwerpen/nationaal-dreigingsbeeld/2017/nationaal-dreigingsbeeld-2017.pdf*.

Bosman, J.; Gijsen, B.M.M. "Evolution of Internet interconnection: Opinion paper." Den Haag: TNO, 2020. http://resolver.tudelft.nl/uuid:38f93a1c-6e20-413d-a7fd-cc6919a7e348.

Bouffard, Benoit; Pernet-Mugnier, Leo. "What are the trends and challenges in industrial cybersecurity in 2021?" RiskInsight (oktober 2021). *https://www.riskinsight-wavestone.com/en/2021/10/what-are-the-trends-and-challenges-in-industrial-cybersecurity-in-2021/*.

Brooks, Chuck. "3 Key Cybersecurity Trends To Know For 2021 (and On ...)." Forbes (12 april 2021). *https:// www.forbes.com/sites/chuckbrooks/2021/04/12/3-key-cybersecurity-trends-to-know-for-2021-and-on-/?sh=7d4a08374978*.

Cimpanu, Catalin. "Four years after the Dyn DDoS attack, critical DNS dependencies have only gone up." ZDNet (30 november 2020). *https:// www.zdnet.com/article/four-years-after-the-dyn-ddos-attack-critical-dns-dependencies-have-only-gone-up/.*

Cyber Security Raad. "'Digitale autonomie Nederland staat onder druk'." Cyber Security Raad (14 mei 2021). *https://www.cybersecurityraad.nl/actueel/nieuws/2021/05/14/%E2%80%98digitale-autonomie-nederland-staat-onder-druk%E2%80%99*.

Davids, Marco. "Goede dingen hebben tijd nodig: Een update over onze publieke NTP-dienst TimeNL." SIDN Labs (19 april 2021). *https://www.sidnlabs.nl/nieuws-en-blogs/goede-dingen-hebben-tijd-nodig*.

Dixon, William; Eagan, Nicole. "3 ways AI will change the nature of cyber attacks." World Economic Forum (19 juni 2019). *https://www.weforum.org/agenda/2019/06/ai-is-powering-a-new-generation-of-cyberattack-its-also-our-best-defence/*.

Europol. *European Union Serious and Organised Crime Threat Assessment (SOCTA) 2021. A corrupting influence: the infiltration and understanding and undermining of Europe's economy and society by organised crime*. Luxembourg: Publications Office of the European Union, 2021. https://*www.europol.europa.eu/publication-events/main-reports/european-union-serious-and-organised-crime-threat-assessment-socta-2021*.

Europol. *Internet Organised Crime Threat Assessment (IOCTA)* 2020. Luxembourg: Publications Office of the European Union, 2020. *https://www.europol.europa.eu/publications-events/main-reports/internet-organised-crime-threat-assessment-iocta-2020*.

FBI Cyber Division. "TRITON Malware Remains Threat to Global Critical Infrastructure Industrial Control Systems (ICS)." 24 maart 2022. *https://www.ic3.gov/Media/News/2022/220325.pdf*.

GFCE meeting "Trends in Cyber Crime" (22 september 2021).

Giles, Martin. "Triton is the world's most murderous malware, and it's spreading." MIT Technology Review (5 maart 2019). *https://www.technologyreview.com/2019/03/05/103328/cybersecurity-critical-infrastructure-triton-malware/*.

Global Encryption Coalition. "Internet Society Open Letter Against Lawful Access to Encrypted Data Act." Global Encryption Coalition (7 juli 2020). *https://www.globalencryption.org/2020/07/internet-society-open-letter-against-lawful-access-to-encrypted-data-act/*.

Greenberg, Andy. "A guide to LockerGoga, the Ransomware Crippling Industrial Firms." Wired (25 maart 2019). *https://www.wired.com/story/lockergoga-ransomware-crippling-industrial-firms/*.

Greenberg, Andy. "A Hacker Tried to Poison a Florida City's Water Supply, Officials Say." Wired (8 februari 2021). *https://www.wired.com/story/oldsmar-florida-water-utility-hack/*.

Greenberg, Andy. "The Untold Story of NotPetya, the Most Devastating Cyberattack in History." Wired (22 augustus 2018). *https://www.wired.com/story/notpetya-cyberattack-ukraine-russia-code-crashed-the-world/*.

Guembe, Blessing; Azeta, Ambrose; Misra, Sanjay; Chukwudi Osamor, Victor; Fernandez-Sanz, Luis; Pospelova, Vera. "The Emerging Threat of Ai-driven Cyber Attacks: A Review." *Applied Artificial Intelligence* (2022): 1-34. *https://doi.org/10.1080/08839514.2022.2037254*.

Halderen, Berry van; Rijswijk-Deij, Roland van. "Supporting DNSSEC Key Signing Ceremonies." NLNet

Labs (1 december 2020). *https://blog.nlnetlabs.nl/supporting-dnssec-key-signing-ceremonies/*.

ICANN Research. "TLD DNSSEC Report." *http://stats.research.icann.org/dns/tld_report/*.

Internet Society. "Internet Invariants: What Really Matters." Public Policy Brief (26 september 2016). *https://www.internetsociety.org/wp-content/uploads/2017/09/ISOC-PolicyBrief-InternetInvariants-20160926-nb.pdf*.

Janardhan, Santosh. "More details about the October 4 outage." Engineering at Meta (5 oktober 2021). *https://engineering.fb.com/2021/10/05/networking-traffic/outage-details/*.

Janardhan, Santosh. "Update about the October 4th outage." Engineering at Meta (4 oktober 2021). *https://engineering.fb.com/2021/10/04/networking-traffic/outage/*.

Kashaf, Aqsa; Sekar, Vyas; Agarwal,Yuvraj. "Analyzing Third Party Service Dependencies in Modern Web Services: Have We Learned from the Mirai-Dyn Incident?." *IMC '20, Virtual Event* (27-29 oktober 2020). *https://dl.acm.org/doi/pdf/10.1145/3419394.3423664*.

KIVI webinar "Terugblik op Trends in Cybersecurity" (8 september 2021).

Koomen, Maria. "The Encryption Debate in the European Union: 2021 Update." *Carnegie Endowment for International Peace International Encryption Brief* (31 maart 2021). *https://carnegieendowment.org/2021/03/31/encryption-debate-in-european-union-2021-update-pub-84217*.

Korolov, Maria; Korolov, Alex. "Top 10 outages of 2021." Network World (31 januari 2022). *https://www.networkworld.com/article/3648352/top-10-outages-of-2021.html*.

Laconi, Paolo. "Zo kwam Europa's grootste datacentrum in een polder bij Zeewolde." De Stentor (23 januari 2022). *https://www.destentor.nl/zeewolde/zo-kwam-europas-grootste-datacentrum-in-een-polder-bij-zeewolde~a82dbd49/*.

Landi, Heather. "Report: 40% of healthcare organizations hit by WannaCry in past 6 months." Fierce Healthcare (29 mei 2019), *https://www.fiercehealthcare.com/tech/lingering-impacts-from-wannacry-40-healthcare-organizations-suffered-from-attack-past-6-months*.

Lee, Edward A. "Cyber physical systems: Design challenges." *11th IEEE international symposium on object and component-oriented real-time distributed computing* (ISORC) (mei 2008): 363-369. 10.1109/ISORC.2008.25.

Lella, Ifigeneia; Theocharidou, Marianthi; Tsekmezoglou, Eleni; Malatras, Apostolos; Garcia, Sebastian; Valeros, Veronica, ed. *ENISA Threat Landscape for Supply Chain Attacks*. European Union Agency for Cybersecurity, 2021. *https://www.enisa.europa.eu/publications/threat-landscape-for-supply-chain-attacks*.

Lewis, Dave. "The DDoS Attack Against Dyn One Year Later." Forbes (23 oktober 2017). *https://www.forbes.com/sites/davelewis/2017/10/23/the-ddos-attack-against-dyn-one-year-later/?sh=2f8f96991ae9*.

Martinho, Celso; Strickx, Tom. "Understanding How Facebook Disappeared from the Internet." Cloudflare (4 oktober 2021). *https://blog.cloudflare.com/october-2021-facebook-outage/*.

Mathew, Alex. "Network Slicing in 5G and the Security Concerns." *Proceedings of the Fourth International Conference on Computing Methodologies and Communication (ICCMC 2020)*. 10.1109/ICCMC48092.2020.ICCMC-00014.

McPherson, D. "Routing Without Rumor. Securing the Internet's Routing System." In: *New Conditions and Constellations in Cyber, Cyberstability Paper Series*. Ed. A. Klimberg. Den Haag: The Hague Centre for Strategic Studies, 2021. 77-91. *https://cyberstability.org/wp-content/uploads/2021/12/Cyberstability-Paper-Series.pdf*.

Modderkolk, Huib. "'Hello, need data back? Contact us fast. Hackers eisen geld van gemeente Hof van Twente." De Volkskrant (7 december 2020). *https://www.volkskrant.nl/nieuws-achtergrond/hello-need-data-back-contact-us-fast-hackers-eisen-geld-van-gemeente-hof-van-twente~b6c46cff/*.

Müller, Moritz; de Jong, Jins; van Heesch, Maran; Overeinder, Benno; van Rijswijk-Deij, Roland. "Retrofitting post-quantum cryptography in Internet protocols: A case study of DNSSEC." *ACM SIGCOMM Computer Communication Review* 50, no.4 (oktober 2020): 49-57. *https://www.sidnlabs.nl/downloads/7qGFWoDiOkovovWyDK9qaK/de709198ac34477797b381f146639e27/Retrofitting_Post-Quantum_Cryptography_in_Internet_Protocols.pdf*.

NCSC. *Cybercrime, van herkenning tot aangifte* (Den Haag: NCSC, 2012). *https://www.ncsc.nl/documenten/publicaties/2019/juli/18/handreiking-cybercrime*.

NCSC. "ICS/SCADA." *https://www.ncsc.nl/onderwerpen/ics*.

NCSC. Maandmonitor november 2021.

NCTV. *Cybersecuritybeeld Nederland* (CSBN) 2020. Den Haag: 2020. *https://www.ncsc.nl/documenten/publicaties/2020/juni/29/csbn-2020*

NCTV. *Cybersecuritybeeld Nederland* (CSBN) 2021. Den Haag: 2021. *https://www.nctv.nl/documenten/publicaties/2021/06/28/cybersecuritybeeld-nederland-2021*.

NCTV. "Overzicht vitale processen." *https://www.nctv.nl/onderwerpen/vitale-infrastructuur/overzicht-vitale-processen*.

Newman, Lily Hay. "Ransomware Hits Dozens of Hospitals in an Unprecedented Wave." Wired (29 oktober 2020). *https://www.wired.com/story/ransomware-hospitals-ryuk-trickbot/*.

Newman, Lily Hay. "The Ransomware Meltdown Experts Warned About Is Here." Wired (12 mei 2017). *https://www.wired.com/2017/05/ransomware-meltdown-experts-warned/*.

NOS. "Hackers Universiteit Maastricht zaten maanden in netwerk; 200.000 euro betaald." NOS Nieuws (5 februari 2020). *https://nos.nl/artikel/2321732-hackers-universiteit-maastricht-zaten-maanden-in-netwerk-200-000-euro-betaald*.

NOS. "'Kaas-hack' opgelost, ging om gijzelsoftware." NOS Nieuws (12 april 2021). *https://nos.nl/artikel/2376425-kaas-hack-opgelost-ging-om-gijzelsoftware*.

Olimid, Ruxandra F.; Nencioni, Gianfranco. "5G Network Slicing: A Security Overview." *IEEE Access* 8 (mei 2020). *https://ieeexplore.ieee.org/stamp/stamp.jsp?arnumber=9099823*.

Olmstead, Kenneth; Polk, Ryan. "Latest U.S. 'Anti-Encryption' Bill Threatens Security of Millions." Internet Society (7 juli 2020). *https://www.internetsociety.org/blog/2020/07/latest-u-s-anti-encryption-bill-threatens-security-of-millions/*.

Osborne, Charlie. "This is how EKANS ransomware is targeting industrial control systems." ZDNet (2 juli 2020). *https://www.zdnet.com/article/this-is-how-ekans-ransomware-is-targeting-industrial-control-systems/*.

Quantum vision team. "Quantum Internet: The internet's next big step." *Issuu* (3 juni 2019). *https://issuu.com/tudelft-mediasolutions/docs/quantum_magazine_june_2019*.

Rijksoverheid. "EU-ministers akkoord met regelgeving voor digitale diensten en markten." Rijksoverheid (25 november 2021). *https://www.rijksoverheid.nl/actueel/nieuws/2021/11/24/eu-ministers-akkoord-met-regelgeving-digitale-diensten-en-markten*.

Root Zone KSK Operator Policy Management Authority. "DNSSEC Practice Statement for the Root Zone KSK Operator." IANA (4 november 2020). *https://www.iana.org/dnssec/procedures/ksk-operator/ksk-dps-20201104.html*

"RPKI documentation." RPKI. Geraadpleegd op 10 juni 2022, *https://rpki.readthedocs.io/en/latest/*.

Ruijven, Theo van; Duijnhoven, Hanneke; Overeinder, Benno; Akkerhuis, Jaap. "ANV Verkenning t.b.v. de risicocategorie Aantasten functioneren Internet." *DHW-NO-TNO 2018 R10331*. Den Haag: TNO/NLnet Labs, 2018.

Schellevis, Joost; Meindertsma, Ben. "Zeker vijftien ziekenhuizen geïnfecteerd met ransomware." NOS Nieuws (25 juni 2017), *https://nos.nl/artikel/2179941-zeker-vijftien-ziekenhuizen-geinfecteerd-met-ransomware*.

Shor, Peter W. "Polynomial Time Algorithms for Discrete Logarithms and Factoring on a Quantum Computer." *SIAM J.Sci.Statist.Comput.* 26 (1997): 1-28. *https://doi.org/10.48550/arXiv.quant-ph/9508027*.

Slayton, Thomas B. "Ransomware: The Virus Attacking the Healthcare Industry." *Journal of Legal Medicine 38*, no. 2 (April 2018): 287-311. *https://doi.org/10.1080/01947648.2018.1473186*.

Stoecklin, Marc Ph.; Jang, Jiyong; Kirat, Dhilung. "DeepLocker: How AI Can Power a Stealthy New Breed of Malware." SecurityIntelligence (8 augustus 2018). *https://securityintelligence.com/deeplocker-how-ai-can-power-a-stealthy-new-breed-of-malware/*.

Taylor, Amiah. "There's a huge surge in hackers holding data for ransom, and experts want everyone to take these steps." Fortune (17 februari 2022). *https://fortune.com/2022/02/17/ransomware-attacks-surge-2021-report/*.

Truong Thanh, Cong; Zelinka, Ivan. "A survey on Artificial Intelligence in Malware as Next-Generation Threats." *Mendel* 25, no. 2 (2019): 27-34. *https://doi.org/10.13164/mendel.2019.2.027*.

Turton, W.; Mehrotra K. "Colonial Pipeline Cyber Attack: Hackers Used Compromised Password." Bloomberg (4 juni 2021). *https://www.bloomberg.com/news/articles/2021-06-04/hackers-breached-colonial-pipeline-using-compromised-password#xj4y7vzkg*.

Vegelien, Stephan. "Nederlandse zeekabels verouderen: 'Digitale sleutelpositie in gevaar'." Tweakers (15 juni 2021). *https://tweakers.net/reviews/9070/all/nederlandse-zeekabels-verouderen-digitale-sleutelpositie-in-gevaar.html*.

Vigliarolo, Brandon. “Local governments continue to be the biggest target for ransomware attacks.” TechRepublic (27 augustus 2020). *https://www.techrepublic.com/article/local-governments-continue-to-be-the-biggest-target-for-ransomware-attacks/*.

Voge, Callum. “UK Online Safety Bill Set to Weaken Encryption and Put UK Internet Users At Risk.” Internet Society (19 januari 2022). *https://www.internetsociety.org/blog/2022/01/uk-online-safety-bill-set-to-weaken-encryption-and-put-uk-internet-users-at-risk/*.

Wan, Adrian. “ISPs Should Strongly Consider MANRS to Fight Cybercrime: World Economic Forum Report.” MANRS (23 januari 2020). *https://www.manrs.org/2020/01/isps-should-strongly-consider-manrs-to-fight-cybercrime-wef-report/*.

Waterfall. “The Top 20 Cyber Attacks on Industrial Control System.” Waterfall Security (2018). *https://waterfall-security.com/20-attacks/*.

Weerd, Carolina van; Lassche, Deborah “National Security Implications of Quantum Technology and Biotechnology.” *Strategic Alert HCSS & TNO* (oktober 2021). *https://publications.tno.nl/publication/34638911/49Bqnv/weerd-2021-national.pdf*.

Wijngaards, Wouter C.A.; Overeinder, Benno J. “Securing DNS: Extending DNS servers with a DNSSEC validator.” *IEEE Security & Privacy* 7, no. 5 (oktober 2009): 36-43. 10.1109/MSP.2009.133.

Williams, Shannon. “Ransomware topped ICS and OT threats in 2021 – report.” Securitybrief (3 maart 2022). *https://securitybrief.co.nz/story/ransomware-topped-ics-and-ot-threats-in-2021-report*.

World summit on the information society. *Tunis Agenda for the Information Society*. WSIS-05/TUNIS/DOC/6(Rev. 1)-E (november 2005). *https://www.itu.int/net/wsis/docs2/tunis/off/6rev1.html*.

“Z-CERT waarschuwt voor mogelijke opmars ransomware.” ICT&health (5 november 2020). *https://www.icthealth.nl/nieuws/z-cert-waarschuwt-voor-mogelijke-opmars-ransomware/*.

Zetter, Kim. “An Unprecedented Look at Stuxnet, the World’s First Digital Weapon.” Wired (3 november 2014). *https://www.wired.com/2014/11/countdown-to-zero-day-stuxnet*.

Zetter, Kim. “Inside the Cunning, Unprecedented Hack of Ukraine’s Power Grid.” Wired (3 maart 2016). *https://www.wired.com/2016/03/inside-cunning-unprecedented-hack-ukraines-power-grid/*.

Bijlage 1 Deelnemende organisaties expertsessies

Voor deze analyse zijn expertsessies gehouden waar deelnemers van de volgende organisaties bij betrokken waren.

Deelnemende organisaties

- AIVD
- Defensie
- FOX-IT
- HSD
- I&W
- ISOC
- KPN
- M&I/partners
- NLnet Labs
- SIDN Labs
- TNO
- Universiteit Twente
- Z-CERT

Rijksoverheid

Analistennetwerk Nationale Veiligheid
redactie: TNO

Dit is een uitgave van:

Het Rijksinstituut voor Volksgezondheid en Milieu (RIVM)
Nederlandse Organisatie voor toegepast-natuurwetenschappelijk onderzoek (TNO)
Stichting Nederlands Instituut voor Internationale Betrekkingen 'Clingendael' (Clingendael)
SEO Economisch Onderzoek (SEO)
Algemene Inlichtingen- en Veiligheidsdienst (AIVD)
Militaire Inlichtingen- en Veiligheidsdienst (MIVD)
Wetenschappelijk Onderzoek- en Documentatiecentrum (WODC)

juli 2022

012454