Nationaal Cyber Security Centrum
Ministerie van Justitie en Veiligheid

Dreigingsscenario’s voor Nederland in relatie tot de oorlog in Oekraïne

Update, december 2022

Publicatiedatum: 1 december 2022

Toegestane verspreiding van TLP: AMBER
(Traffic Light Protocol)

Deze dreigingsanalyse bevat het label TLP: AMBER en wordt door het NCSC verspreid. Het NCSC gebruikt het Traffic Light Protocol (TLP) om eenduidig te definiëren wat er met de informatie mag gebeuren. Wanneer informatie is voorzien van een TLP-aanduiding weet u met wie u deze informatie mag delen. Dit staat beschreven in de standaard First (www.first.org/tlp). Deze dreigingsanalyse is te gebruiken binnen uw organisatie, te delen met collega’s of externe partijen zoals klanten op basis van *need-to-know* zodat zij zich kunnen beschermen of verdere schade kan worden voorkomen. Het is echter niet de bedoeling dat u de informatie publiek maakt.

Uw reacties zijn welkom op info@ncsc.nl

Inhoud

Inleiding

Het Nationaal Cyber Security Centrum (NCSC) is het centrale informatieknooppunt en expertisecentrum voor cybersecurity in Nederland. Deze positie stelt het NCSC in staat om op nationaal niveau te kijken naar digitale dreigingen en bij te dragen aan het vergroten van de weerbaarheid van de Nederlandse samenleving in het digitale domein.

Update december 2022

In februari en april 2022 heeft het NCSC de analyse "Dreigingsscenario's voor Nederland in relatie tot de oorlog in Oekraïne" uitgebracht met als doel het digitale dreigingslandschap voor Nederlandse overheidsorganisaties en vitale sectoren in kaart te brengen. Hierna zijn in juli en augustus twee verdiepende analyses gepubliceerd over respectievelijk digitale spionage en hacktivisme.

In deze laatste update wordt teruggeblikt op de scenario’s die begin 2022 zijn opgesteld en worden de waarschijnlijkheidsinschattingen waar nodig bijgesteld met het oog op 2023. Dit doet het NCSC op basis van eigen waarnemingen van de afgelopen maanden en eigen inschattingen met betrekking tot factoren gelieerd aan het conflict die van invloed (kunnen) zijn op het handelen van actoren. In bijlage E is een selectie te vinden van incidenten en meldingen die hierin zijn meegenomen. In deze analyse is ook gebruik gemaakt van inzichten van de AIVD en de MIVD.

Deze publicatie dient om de Nederlandse Rijksoverheid en organisaties in vitale sectoren handvatten te geven om zelfstandige dreigingsanalyses uit te voeren en te helpen bij een afweging omtrent te nemen maatregelen. Een dreigingsanalyse vormt samen met een belangen- en weerbaarheidsanalyse van uw organisatie de bouwstenen voor risicomanagement.

Het dreigingslandschap ten aanzien van de oorlog in Oekraïne blijft volatiel en divers. Ook omdat veel van de waargenomen activiteiten zich voornamelijk concentreren op Oekraïne en de directe buurlanden, moet rekening gehouden worden met een

aanzienlijke onzekerheidsmarge in de inschattingen van het NCSC voor Nederlandse organisaties. Daar komt bij dat het NCSC geen volledig beeld heeft op alle aanvallen die plaatsvinden in het digitale domein. Organisaties kunnen bijdragen aan een volledig dreigingsbeeld door relevante informatie met het NCSC te delen.

Het NCSC blijft waakzaam voor veranderingen aangaande het dreigingsbeeld en adviseert organisaties alert te blijven en het geboden handelingsperspectief op te volgen. Het NCSC staat eveneens in contact met (inter)nationale partners en doelgroepen om nieuwe informatie snel te duiden en te delen.

Samenvatting

- Deze analyse bouwt voort op eerdere publicaties in februari en april van dit jaar. In deze update is het **meest recente dreigingsbeeld** opgenomen voor Nederland in relatie tot de oorlog in Oekraïne. De scenario's zijn gebaseerd op waargenomen digitale aanvallen (bijlage E), verrijkt met inzichten van het NCSC en nationale partners.

- Deze publicatie biedt organisaties **handvatten om zelfstandige risicoanalyses uit te voeren** en te helpen bij een afweging omtrent te nemen maatregelen. Hier kunnen ook inzichten uit het handelingsperspectief gebruikt worden, alsmede de TTP's van relevante actoren.

- De focus van actoren lijkt primair te liggen op Oekraïne en Rusland zelf en in de tweede plaats op de directe buurlanden van Oekraïne. Hierdoor valt de dreigingsappreciatie op een aantal punten lager uit dan eerder verwacht. **Waakzaamheid blijft echter geboden** gezien de aanhoudende spanningen tussen Rusland en het Westen.

- Actoren kunnen snel hun focus verleggen en doelstellingen aanpassen op basis van actuele gebeurtenissen. Daar komt bij dat de **weerbaarheid** van organisaties direct **gekoppeld** lijkt **aan doelwitselectie** van (vaak opportunistisch) handelende actoren.

- Zo blijft **digitale sabotage** ook in Nederland **een scenario waar rekening mee gehouden moet worden**. Hierbij moet ook gedacht worden aan de inzet van ransomware/wiperware. Digitale sabotage hoeft overigens niet gericht te zijn op langdurige ontwrichting, maar kan ook bedoeld zijn om een **psychologisch effect** teweeg te brengen. Een digitale aanval met beperkte impact op een kleinere (keten)organisatie kan hiervoor voldoende zijn.

- Naast statelijke actoren spelen **hacktivisten** een actieve rol op het gebied van digitale offensieve activiteiten. **DDoS-aanvallen** voerden wat dit betreft de boventoon, hoewel de frequentie lijkt te zijn afgenomen. Een deel van de hacktivisten kan ook na het conflict actief blijven.

- Hacktivisten richten zich ook op het **verstoren van de informatievoorziening van overheidsinstanties**. Hoewel voornamelijk symbolisch van aard, kunnen deze wel degelijk een (tijdelijk) verstorend effect hebben.

- Daar komt bij dat **overheden en/of overheidsinstanties**, naast organisaties binnen de vitale sector, rekening moeten houden met (mogelijk politiek-gemotiveerde) **ransomware-aanvallen**.

- Verder blijven **digitale spionageactiviteiten gericht op politiek-strategische inzichten** een belangrijke dreiging. Hoewel deze niet direct een relatie hoeven te hebben met de oorlog in Oekraïne, kunnen ontwikkelingen hieromtrent wel een effect hebben op de omvang en intensiteit van deze activiteiten.

- Ook is het mogelijk dat Rusland afhankelijker wordt van **digitale spionage ten behoeve van economische doeleinden**, bijvoorbeeld op het gebied van hoogwaardige technologie.

Scenario's en waarschijnlijkheidsinschattingen

			Waarschijnlijkheid per conflictstadium*		
			Voortzetting van de oorlog	Staakt-het-vuren	Vredes-overeenkomst
Dreigingsscenario's	1A	Verstoringen van logistieke processen	Mogelijk —	Onwaarschijnlijk ↓	Onwaarschijnlijk ↓
	1B	Verstoringen van communicatieverkeer	Twijfelachtig ↓	Onwaarschijnlijk ↓	Onwaarschijnlijk —
	1C	Verstoringen in een energienetwerk	Mogelijk —	Twijfelachtig ↓	Twijfelachtig —
	1D	Verstoringen van betalingsverkeer	Twijfelachtig ↓	Onwaarschijnlijk ↓	Onwaarschijnlijk —
	1E	Aantasting waterbeheer	Onwaarschijnlijk —	Onwaarschijnlijk —	Onwaarschijnlijk —
	2A	Een ongecontroleerd cyberwapen	Twijfelachtig ↓	Onwaarschijnlijk ↓	Onwaarschijnlijk —
	2B	Opportunistische meelifters	Waarschijnlijk —	Mogelijk —	Mogelijk —
	2C	Niet-statelijke actoren met ideologisch/politieke motieven (hacktivisme)	Mogelijk ↓	Twijfelachtig —	Twijfelachtig ↑
	3	Digitale spionageactiviteiten door statelijke actoren	Waarschijnlijk —	Waarschijnlijk —	Waarschijnlijk —
	4A	Desinformatie via gecompromitteerde accounts	Twijfelachtig —	Twijfelachtig —	Twijfelachtig —
	4B	Defacement-aanvallen en aantasting van online beschikbare informatie	Twijfelachtig —	Onwaarschijnlijk ↓	Onwaarschijnlijk —
	4C	Hack-en-lek operaties met een politiek motief	Twijfelachtig ↓	Twijfelachtig —	Twijfelachtig —
	4D	*Nieuw scenario*: Verstoring van informatievoorziening overheidsinstanties	Mogelijk	Twijfelachtig	Twijfelachtig
	5	Statelijke economische spionage	Mogelijk ↑	Mogelijk —	Mogelijk —
	6	Digitale aanvallen voor financieel gewin	Waarschijnlijk —	Waarschijnlijk —	Waarschijnlijk —

**Waarschijnlijkheid dreigingsscenario's voor Nederland. Het symbool "↑" houdt in dat een inschatting ten opzichte van de laatste update in april 2022 naar boven is bijgesteld. Het symbool "↓" houdt in dat een inschatting naar beneden is bijgesteld. Inschattingen met een "—" zijn ongewijzigd. Zie voor meer informatie Bijlage A.*

Dreigingsscenario's

Dreigingscategorie 1: Doelgerichte digitale aanvallen gericht op sabotage van vitale infrastructuur

Digitale aanvallen binnen deze categorie zijn gerichte digitale aanvallen met het oog op sabotage van vitale infrastructuur in Nederland.[1] Ondanks dat in het conflict minder verstorende aanvallen hebben plaatsgevonden dan geanticipeerd, dient men rekening te blijven houden met de mogelijkheid tot digitale sabotage. De kans op een ontwrichtende digitale aanval wordt binnen de huidige context enigszins hoger ingeschat voor logistieke processen en de energiesector. Voor andere sectoren is deze naar beneden bijgesteld. Dergelijke aanvallen hoeven niet per definitie een significante operationele impact te hebben of gericht te zijn op langdurige ontwrichting, maar kunnen ook tot doel hebben een psychologisch effect teweeg te brengen. Kleinere (keten)organisaties kunnen daarom ook een interessant doelwit vormen. De weerbaarheid van organisaties speelt een belangrijke rol wat betreft doelwitselectie. Hierbij moet ook de inzet van ransomware/wiperware in acht worden genomen.

Mogelijke ontwrichtende aanvallen

In de huidige fase van het conflict voert digitale spionage en beïnvloeding (zoals desinformatie) de boventoon. Desalniettemin is het ook mogelijk dat digitale aanvallen ontwrichtend kunnen werken.[2] Over het algemeen vergen dergelijke aanvallen, gericht op bijvoorbeeld operationele processen, een intensieve voorbereiding, capaciteit en tijd. In eerste instantie betekent dit vaak dat actoren zich prepositioneren of innestelen om

[1] Ook verstoringen van vitale processen bij naburige landen kunnen, door onderlinge afhankelijkheden, aanzienlijke effecten hebben op Nederland. Keteneffecten worden gedeeltelijk behandeld onder categorie 2.

[2] https://www.ncsc.nl/onderwerpen/oekraine-aivd-mivd

eventueel op een later moment over te kunnen gaan op sabotage.[3] Ook de inzet van ransom- en wiperware kan leiden tot verstoring van operationele processen. [4]

Binnen dit kader moet ook worden uitgegaan van opportunisme wat betreft doelwitselectie. De weerbaarheid van organisaties speelt hierin een grote rol. Hoe lager de drempel, hoe makkelijker het is voor kwaadwillenden om toegang te krijgen tot een netwerk of systeem. Organisaties moeten daarom ook rekening houden met reconnaissance-activiteiten. Hierbij wordt bijvoorbeeld gescand op kwetsbaarheden of openstaande poorten.[5] Ook is sabotage niet per definitie gericht op langdurige ontwrichting. Dergelijke digitale aanvallen kunnen ook gericht zijn op het teweegbrengen van een psychologisch effect en het uitvoeren van druk op besluitvorming. Een digitale aanval met beperkte impact kan namelijk het signaal afgeven dat een actor over de middelen beschikt om in een later stadium mogelijk een aanval met een daadwerkelijk ontwrichtende werking uit te voeren. Enige terughoudendheid vanuit Russische statelijke actoren lijkt eveneens aannemelijk om verdere escalatie te voorkomen. Ook kleinere (keten)organisaties kunnen daarom een interessant doelwit vormen. Bovenstaande kanttekeningen vergroten de onzekerheidsmarge van de waarschijnlijkheidsinschattingen binnen deze dreigingscategorie.

[3] Zie het Dreigingsbeeld Statelijke Actoren 2: https://www.aivd.nl/documenten/publicaties/2022/11/28/dreigingsbeeld-statelijke-actoren-dbsa-2

[4] Hacktivistische aanvallen worden primair behandeld onder scenario 2C. In het geval van schijnbare compromittatie van OT-systemen door hacktivistische actoren blijkt de daadwerkelijke impact en doelgerichtheid zeer twijfelachtig en opportunistisch van aard. Ook DDoS-aanvallen lijken eerder gericht op het verstoren van digitale dienstverlening (met symbolische impact) dan het daadwerkelijk aantasten van de onderliggende infrastructuur.

[5] https://www.crowdstrike.com/cybersecurity-101/cyber-kill-chain/

		Waarschijnlijkheid per conflictstadium		
		Voortzetting van de oorlog	Staakt-het-vuren	Vredesovereenkomst
1A	Verstoringen van logistieke processen	Mogelijk —	Onwaarschijnlijk ↓	Onwaarschijnlijk ↓
1B	Verstoringen van communicatieverkeer	Twijfelachtig ↓	Onwaarschijnlijk ↓	Onwaarschijnlijk —
1C	Verstoringen in een energienetwerk	Mogelijk —	Twijfelachtig ↓	Twijfelachtig —
1D	Verstoringen van betalingsverkeer	Twijfelachtig ↓	Onwaarschijnlijk ↓	Onwaarschijnlijk —
1E	Aantasting waterbeheer	Onwaarschijnlijk —	Onwaarschijnlijk —	Onwaarschijnlijk —

1A: Verstoringen van logistieke processen

Buiten Nederland zijn in het kader van het conflict in beperkte mate aanvallen op logistieke processen waargenomen. Het gaat in dit geval met name om verstorende DDoS-aanvallen op websites van logistieke dienstverleners door niet-statelijke actoren. Vermeende aanvallen op OT-processen kunnen niet of nauwelijks worden bevestigd. Ook de mogelijke inzet van een wiper tegen een controlepost aan de Oekraïense grens met Roemenië lijkt geen navolging te hebben gehad en de daadwerkelijke impact hiervan blijft ongewis. In november bericht Microsoft over Prestige-ransom/wiperware, een campagne die vanaf maart 2022 actief is en geattribueerd wordt aan de Russische statelijke actor IRIDIUM.[6] De campagne richt zich met name op transportorganisaties in Polen en Oekraïne. Hierbij moet wel opgemerkt worden dat het niet lijkt te gaan om organisaties binnen de vitale sector en dat de impact van de campagne waarschijnlijk beperkt is. De dreiging tegen andere organisaties die verantwoordelijk zijn voor het leveren van militaire of humanitaire hulp aan Oekraïne neemt hierdoor volgens Microsoft wel toe.

Door het uitblijven van abrupte troepenopbouw vanuit het Westen of grootschalige verplaatsing van materieel via Nederland, lijkt het belang van het mogelijk aanvallen van logistieke punten, zoals de haven van Rotterdam, te zijn afgenomen. Toch kan het

[6] De IRIDIUM-groep heeft overlap met Sandworm. Zie: https://www.microsoft.com/en-us/security/blog/2022/10/14/new-prestige-ransomware-impacts-organizations-in-ukraine-and-poland/

scenario met betrekking tot ontwrichting hiervan niet worden uitgesloten. De nadruk vanuit Rusland op wapenleveranties vanuit het Westen in combinatie met waargenomen activiteiten, zoals hierboven beschreven, dragen bij aan de inschatting dat verstoring van logistieke processen **mogelijk blijft**. Nogmaals, het kan hierbij ook gaan om een digitale aanval met symbolische impact. Kleinere, bijvoorbeeld logistieke, (keten)partijen kunnen hiervan ook slachtoffer worden. Bij verminderende spanningen, zoals in het geval van een vredesakkoord, loopt de waarschijnlijkheid snel af naar onwaarschijnlijk aangezien hierdoor de noodzaak tot dergelijke acties afneemt.

Nota bene, logistieke processen blijven eveneens een interessant doelwit voor niet-statelijke actoren voor financieel gewin (zie categorie 6).

1B: Verstoringen van datacommunicatie

Sinds de start van de oorlog hebben zich buiten Nederland enkele incidenten voorgedaan waarbij datacommunicatie is verstoord. Hoewel er geen aanwijzingen zijn dat het raken van Oekraïense datacommunicatie in prioriteit is gedaald, werden de meeste succesvolle aanvallen in de eerste maanden van de oorlog uitgevoerd. Hierbij zijn ook keteneffecten waargenomen.[7] CERT-UA waarschuwde op 24 juni 2022 ook voor digitale aanvallen op telecombedrijven in Oekraïne, waarbij gebruik wordt gemaakt van e-mails met een malafide bijlage.[8] Het verstoren van Nederlandse datacommunicatie lijkt op dit moment echter niet de intentie van bij het conflict betrokken actoren. Wel dient men rekening te houden met de mogelijkheid van spillover-effecten, onder andere via eventuele opportunistische aanvallen vanuit hacktivistische hoek.[9] Dit ligt echter momenteel niet in de lijn der verwachting. Digitale verstoring van communicatie-infrastructuur op Nederlands grondgebied en van Nederlandse organisaties bij een voortzetting van het conflict is in deze update dan ook **naar beneden bijgesteld van mogelijk naar twijfelachtig**. Naarmate de spanningen verminderen, neemt ook de waarschijnlijkheid af. In het geval van verdere internationale escalatie moet ook rekening gehouden

[7] Zie hiervoor bijlage E van de "Dreigingsscenario's voor Nederland in relatie tot de oorlog in Oekraïne" (versie 2, april 2022). Zo verloren gelijktijdig met de Russische invasie van Oekraïne op 24 februari 2022 duizenden gebruikers door heel Europa hun internetverbinding. Oorzaak was een digitale aanval op systemen behorende bij de KA-SAT-satelliet: een door Viasat beheerde satelliet die internetverbindingen aanbiedt binnen Europa. Ook waren er in maart 2022 diverse keren meldingen van uitval bij de grote Oekraïense providers Ukrtelecom en Triolan.

[8] https://cert.gov.ua/article/405538 & https://cip.gov.ua/en/news/khakeri-atakuyut-ukrayinskikh-operatoriv-i-provaideriv-telekomunikacii

[9] https://cybernews.com/cyber-war/we-breached-russian-satellite-network-say-pro-ukraine-partisans/

worden met andere scenario's, zoals het verstoren van communicatie tussen NAVO-bondgenoten.

1C: Verstoringen in een energienetwerk

Pogingen tot digitale verstoring van energienetwerken zijn in beperkte mate waargenomen in het conflict. Hierbij springt de afgeslagen aanval op een Oekraïense energiecentrale door Sandworm met CaddyWiper en Industroyer2 het meest in het oog.[10] Gezien de recente kinetische aanvallen op elektriciteitscentrales in Oekraïne, lijkt de verdere noodzaak tot het inzetten van geavanceerde cybermiddelen om het Oekraïense energienetwerk te ontwrichten beperkt.[11]

Onder andere de explosies van de Nord Stream-gaspijpleidingen in oktober 2022 duiden echter wel op een mogelijke intentie van bij het conflict betrokken actoren om energienetwerken in Europa te verstoren. De dreiging op energienetwerken geldt ook digitaal en is mogelijk toepasbaar op Nederland.[12] [13] Bijvoorbeeld vanwege de logistieke rol die wordt vervuld door faciliteiten in de Rotterdamse haven voor de energievoorziening van West-Europa, zeker bij een verdere ontkoppeling van Russische grondstoffen. Het treffen van dergelijke faciliteiten kan een verstorend effect hebben op vitale processen, ook buiten Nederland. Ook moet hierbij rekening gehouden worden met een digitale aanval met beperkte impact, omdat dit al genoeg kan zijn om maatschappelijke onrust te creëren en besluitvorming te beïnvloeden. De waarschijnlijkheid van een digitale aanval op het Nederlands energienetwerk wordt daarom **nog steeds ingeschaald als mogelijk**. Ook de eerder vermelde aanklachten van het Amerikaanse ministerie van Justitie, waarin (pogingen tot) compromittatie van honderden bedrijven binnen de energiesector in meer dan 135 landen om hier op een

[10] Zie hiervoor bijlage E van de "Dreigingsscenario's voor Nederland in relatie tot de oorlog in Oekraïne" (versie 2, april 2022).

[11] https://www.nrc.nl/nieuws/2022/11/01/civiel-object-kan-militair-doel-zijn-a4146972

[12] Zie het Dreigingsbeeld Statelijke Actoren 2: https://www.aivd.nl/documenten/publicaties/2022/11/28/dreigingsbeeld-statelijke-actoren-dbsa-2

[13] Ook maakte RTL onlangs melding van mogelijke interesse van Russische actoren in LNG-terminals in Nederland. Dragos heeft aan het NCSC gemeld dat het hierbij niet gaat om een nieuwe ontwikkeling en dat de informatie aangaande de genoemde actoren betrekking heeft op breder waargenomen reconnaissance activiteiten in Noord- en Centraal-Europa. Ook de premier van Noorwegen waarschuwde onlangs dat Rusland "een reële en ernstige bedreiging" vormt voor de olie- en gasindustrie, zie https://securityaffairs.co/wordpress/137561/cyber-warfare-2/norway-pm-warns-russia-threat.html.

later moment mogelijk over te kunnen gaan op sabotage, onderschrijven dit beeld.[14] De waarschijnlijkheid van dit scenario zal afnemen in het geval van een staak-het-vuren of vredesovereenkomst.

1D: Verstoringen in de financiële sector

De bankensector in Oekraïne en omringende landen heeft de afgelopen maanden te maken gehad met diverse DDoS-aanvallen vanuit hacktivistische hoek. Opvallend is dat volgens Mandiant dergelijke aanvallen in sommige gevallen worden neergezet als vergeldingsacties voor overheidssteun aan Oekraïne. Dergelijke aanvallen lijken echter opportunistisch van aard en zijn slechts in beperkte mate verstorend. Ook zijn er in het afgelopen jaar digitale aanvallen met wiperware waargenomen tegen financiële instellingen in Oekraïne.[15] Ontwrichtende aanvallen buiten Oekraïne door meer geavanceerde actoren lijken niet te passen in het huidige verloop van het conflict en sluiten niet aan bij strategische doelstellingen, al kunnen eventuele vergeldingsacties naar aanleiding van ingestelde sancties door het Westen niet geheel uitgesloten worden. Hierbij moet ook rekening gehouden worden met een eventuele digitale aanval op bredere infrastructuur.[16] Financieel gewin zou eveneens een voorstelbaar motief kunnen zijn naarmate de spanningen langer aanhouden en/of de sancties langer van kracht blijven.[17] Aangezien alternatieven op dergelijke acties aanwezig lijken, zoals het omzeilen van sancties middels cryptocurrencies, lijken dergelijke digitale aanvallen omslachtig van aard.[18] Het NCSC stelt de inschatting van verstorende digitale aanvallen op de financiële sector dan ook **bij van mogelijk naar twijfelachtig.**

[14] https://www.justice.gov/opa/pr/four-russian-government-employees-charged-two-historical-hacking-campaigns-targeting-critical

[15] https://www.csoonline.com/article/3674871/ncsc-chief-warns-uk-organizations-ukraine-s-allies-of-possible-massive-cyberattacks-by-russia.html

[16] https://www.spglobal.com/marketintelligence/en/news-insights/latest-news-headlines/european-banks-remain-key-hacking-target-following-russian-invasion-of-ukraine-72578588

[17] Denk binnen een dergelijk scenario bijvoorbeeld aan de Carbanak-aanvallen gericht op financiële instellingen wereldwijd, waarvan de financiële schade wordt geschat op 1 miljard USD. Zie hiervoor bijlage B van de "Dreigingsscenario's voor Nederland in relatie tot de oorlog in Oekraïne" (versie 1, februari 2022).

[18] https://www.cnbc.com/2022/09/20/treasury-department-russia-avoid-sanctions-using-crypto.html

1E: Aantasting waterbeheer

De waarschijnlijkheidsgraad met betrekking tot de aantasting van de drinkwatervoorziening werd in de eerdere dreigingsscenario's van het NCSC gezien als **onwaarschijnlijk**. Deze inschatting **blijft gehandhaafd**. Er zijn geen aanwijzingen dat het raken van de Nederlandse drinkwatervoorziening beoogd wordt door partijen die betrokken zijn in het conflict, aangezien dit niet aansluit bij strategische, tactische of operationele doelstellingen. Dit geldt uitdrukkelijk niet voor Oekraïne, waar met kinetische middelen watervoorzieningen zijn uitgeschakeld.[19] Dergelijke aanvallen zijn echter niet van toepassing op Nederland. Ook keteneffecten lijken hier niet van toepassing.

[19] https://www.reuters.com/world/europe/russian-attacks-ukraines-water-energy-supplies-particularly-heinous-state-dept-2022-11-01/

Dreigingscategorie 2: Spillover-effecten

Spillover-effecten komen indirect voort uit het conflict en kunnen Nederlandse belangen schaden. Hoewel hiervoor werd gevreesd, is de inzet van een ongecontroleerd cyberwapen uitgebleven. De waarschijnlijkheid dat een dergelijk digitaal wapen op een later moment nog wordt ingezet, is afgeschaald naar twijfelachtig. Het is een stuk waarschijnlijker dat ook Nederlandse organisaties te maken krijgen met opportunistische digitale aanvallen, waarin bijvoorbeeld aan de oorlog gerelateerde thema's worden gebruikt voor phishing. Ook is het nog steeds mogelijk dat Nederland in de toekomst te maken krijgt met gerichte hacktivistische aanvallen, ondanks dat deze tot op heden niet zijn waargenomen in Nederland.

Nevenschade door breed scala aan betrokken actoren

De afgelopen maanden heeft een breed scala aan actoren zich gemengd in het digitale speelveld van de oorlog in Oekraïne, dan wel geprobeerd het conflict te gebruiken om zo hun eigen (mogelijk niet aan het conflict-gerelateerde) doelstellingen te bereiken. Opvallend is de grote rol van hacktivisten die zich vanuit ideologisch of politiek gemotiveerde redenen achter Oekraïne of Rusland scharen. Hoewel de impact van digitale aanvallen vanuit dergelijke actoren varieert, zijn ze nadrukkelijk aanwezig in de informatieoorlog tussen Oekraïne en Rusland. De vraag over mogelijke coördinatie tussen statelijke en niet-statelijke actoren wordt hierbij steeds relevanter, maar blijft ambigu.[20]

Over dreigingscategorie 2C, niet-statelijke actoren met ideologisch/politieke motieven (hacktivisme), heeft het NCSC op 8 september 2022 een analyse uitgebracht ("Hacktivistische activiteiten tijdens de oorlog in Oekraïne"). Het beeld dat deze analyse schetst, is nog steeds van toepassing.

[20] https://www.wsj.com/articles/google-sees-russia-coordinating-with-hackers-in-cyberattacks-tied-to-ukraine-war-11663930801

		Waarschijnlijkheid per conflictstadium		
		Voortzetting van de oorlog	Staakt-het-vuren	Vredesovereenkomst
2A	Een ongecontroleerd cyberwapen	Twijfelachtig ↓	Onwaarschijnlijk ↓	Onwaarschijnlijk —
2B	Opportunistische meelifters	Waarschijnlijk —	Mogelijk —	Mogelijk —
2C	Niet-statelijke actoren met ideologisch/politieke motieven (hacktivisme)	Mogelijk ↓	Twijfelachtig —	Twijfelachtig ↑

2A: Een ongecontroleerd cyberwapen

Hoewel de initiële ongerustheid over de inzet van digitale wapens met mogelijk onvoorziene cascade-effecten enigszins is verminderd, kan dit scenario niet geheel uitgesloten worden. Inzet hiervan zou passen in een scenario waarin verdergaande escalatie leidt tot de wil bredere schade te berokkenen aan de Oekraïense digitale infrastructuur en die van haar bondgenoten. Hier ligt echter ook gelijk de zwakte van deze optie, omdat een ongecontroleerde aanval ook schade kan toebrengen aan Russische belangen zoals bijvoorbeeld het geval was bij NotPetya en BadRabbit in 2017.[21] Ook is het de vraag in hoeverre Russische actoren de capaciteit bezitten voor een dergelijke aanval. Zo maakte HermeticWiper geen gebruik van een zeroday-kwetsbaarheid voor verdere verspreiding, maar van lokale rechten die een gebruiker al heeft (WMI) of van een lijst van standaard gebruikersnamen en wachtwoorden (SMB).[22] NotPetya en WannaCry daarentegen maakten gebruik van de wormable EternalBlue-kwetsbaarheid afkomstig van een lek bij de Amerikaanse inlichtingendienst NSA.[23] [24] Het gebruik van een dergelijke kwetsbaarheid is waarschijnlijk maar eenmalig mogelijk en het is daarom twijfelachtig of Russische actoren bereid zouden zijn dit potente en agressieve middel in te zetten voor een digitale aanval waarvan de gevolgen ongewis zijn.

[21] https://www.reuters.com/article/us-cyber-summit-ukraine-idUSKBN1D02D1

[22] https://www.welivesecurity.com/2022/03/01/isaacwiper-hermeticwizard-wiper-worm-targeting-ukraine/

[23] https://www.theguardian.com/technology/2017/dec/30/wannacry-petya-notpetya-ransomware

[24] https://msrc-blog.microsoft.com/2019/05/30/a-reminder-to-update-your-systems-to-prevent-a-worm/

Vanwege het vooralsnog uitblijven van dit scenario en de bovengenoemde kanttekeningen, wordt de waarschijnlijk van de inzet van een ongecontroleerd cyberwapen **afgeschaald naar twijfelachtig**. Een dergelijk scenario hangt echter ook sterk af van de mate van digitale verbondenheid met Oekraïense digitale dienstverleners die mogelijk zouden kunnen fungeren als doorgeefluik bij een supply chain-aanval.[25] Russische statelijke actoren hebben concrete aanvalspogingen gedaan tegen Oekraïense softwarebedrijven, waarschijnlijk met het creëren van mogelijkheden tot supply chain-operaties als oogmerk.[26]

2B: Opportunistische meelifters

Het opportunistisch inspelen op (geopolitieke) ontwikkelingen is inherent aan cyberdreigingen. Zowel statelijke als niet-statelijke opportunistische meelifters gebruiken de oorlog dan ook als thema om hun doelstellingen te behalen. Google's Threat Analysis Group (TAG) neemt van actoren gelieerd aan China, Iran en Noord-Korea waar dat zij aan de oorlog gerelateerde thema's gebruiken om personen te verleiden een kwaadaardige e-mail te openen en/of op een malafide link te klikken.[27] Aan China gelieerde actoren beogen bijvoorbeeld landen die betrokken zijn bij het conflict in Oekraïne te spioneren.[28] Financieel-gemotiveerde actoren verspreiden phishing-mails en delen vervalste websites, die bijvoorbeeld internationale hulpverleningsorganisaties nabootsen.[29] Ook Nederlandse organisaties kunnen slachtoffer worden van deze actoren. De kans op opportunistische aanvallen in Nederland, gelieerd aan de huidige situatie, wordt daarom **nog steeds ingeschaald als waarschijnlijk**. Bij verminderende spanningen hoeft de waarschijnlijkheid van dit scenario niet direct terug te lopen. Beschikbaar gekomen kwetsbaarheden kunnen nog voor een langere tijd uitgebuit worden. Dit geldt ook voor thema's in de nasleep van het conflict die gebruikt kunnen worden voor phishing-mails of andere aanvalsvormen.

[25] Zo werd NotPetya verspreid via het bedrijf M.E.Doc dat accountancy software levert aan een groot aantal Oekraïense organisaties.

[26] https://blog.talosintelligence.com/attackers-target-ukraine-using-gomet/

[27] https://blog.google/threat-analysis-group/update-on-cyber-activity-in-eastern-europe/

[28] https://www.sentinelone.com/labs/targets-of-interest-russian-organizations-increasingly-under-attack-by-chinese-apts/ & https://www.welivesecurity.com/2022/03/23/mustang-panda-hodur-old-tricks-new-korplug-variant/

[29] https://cert.gov.ua/article/987552, https://cert.gov.ua/article/1545776 & https://blog.google/threat-analysis-group/update-on-cyber-activity-in-eastern-europe/

2C: Niet-statelijke actoren met ideologisch/politieke motieven (hacktivisme)

In de eerste weken van de oorlog zijn veel hacktivistische aanvallen waargenomen. Vele hacktivisten en criminelen in het digitale domein hebben partij gekozen en aanvallen uitgevoerd op organisaties in landen die direct of indirect betrokken zijn bij de oorlog.[30] Het gaat hierbij bijvoorbeeld om DDoS-aanvallen, defacements, hack-en-lek operaties en in mindere mate om de inzet van wiperware (eventueel in combinatie met het lekken van gestolen data).[31] Vooral DDoS-aanvallen voeren de boventoon. In de loop der tijd lijkt de frequentie van hacktivistische aanvallen wel te zijn afgenomen, mogelijk omdat een deel van de actoren interesse heeft verloren.[32] Een deel is echter nog steeds actief en deze hacktivisten voeren nog steeds geregeld aanvallen uit. De vorm en impact hiervan is divers, omdat groepen variëren in professionaliteit en vaak van wisselende samenstelling zijn. Pro-Russische hacktivisten formeren en coördineren zichzelf bijvoorbeeld vaak via Telegram. Daar publiceren zij lijsten met doelwitten en roepen gelijkgestemden op om mee te doen met een DDoS-campagne. Pro-Russische hacktivisten richten hun pijlen regelmatig op overheidsinstanties en organisaties binnen de vitale sector in landen die Oekraïne steunen.[33] Mandiant gaat er hierbij van uit dat een aantal van deze hacktivisten mogelijk samenwerken met Russische statelijke actoren of als dekmantel worden gebruikt om attributie van digitale aanvallen te bemoeilijken.[34] De precieze band tussen statelijke actoren en niet-statelijke actoren blijft echter onduidelijk.

Het NCSC heeft in Nederland vooralsnog geen gerichte hacktivistische aanvallen waargenomen. Omdat de focus van hacktivisten momenteel dus niet op Nederland ligt, stelt het NCSC de waarschijnlijkheidsinschatting voor dit scenario **naar beneden bij naar mogelijk**. Echter, regelmatig vormt een specifieke politieke of sociale gebeurtenis

[30] Zie hiervoor ook de kamerbrief "Stand van zaken op het gebied van cyber(security) in relatie tot het conflict in Oekraïne" van 11 maart 2022, https://open.overheid.nl/repository/ronl-f9ee031b8a74380266105384266980229c194e8/1/pdf/tk-stand-van-zaken-op-het-gebied-van-cyber-security-in-relatie-tot-het-conflict-in-oekraine.pdf.

[31] Zoals bijvoorbeeld de recente inzet van een niet-herstelbare variant van Somnia-ransomware door de hacktivistische groepering From Russia With Love. Zie de tijdlijn in bijlage E voor meer informatie.

[32] Vu et al. *Getting Bored of Cyberwar: Exploring the Role of the Cybercrime Underground in the Russia-Ukraine Conflict*. (Aug 2022). https://arxiv.org/pdf/2208.10629.pdf en https://securelist.com/ddos-report-q3-2022/107860/

[33] https://www.politico.eu/article/meet-killnet-russias-hacking-patriots-plaguing-europe/

[34] https://www.mandiant.com/resources/blog/gru-rise-telegram-minions

aanleiding om een hacktivistische aanval uit te voeren. Hacktivisten acteren daarin veelal reactief. Als de politieke spanning tussen Rusland en specifiek Nederland oploopt, is waakzaamheid voor hacktivisme daarom extra belangrijk. Indien de oorlog een door beide partijen gedragen staakt-het-vuren of vredesovereenkomst bereikt, zal deze dreiging afnemen tot twijfelachtig. De motivatie voor hacktivisten om één partij te steunen in de oorlog zal dan afnemen. Wel is het zo dat niet elke hacktivist zich direct achter een overeenkomst scharen. Ook zijn spillover-effecten waarschijnlijk waarbij groepen zich op andere hacktivistische thema's zullen richten of overgaan op criminele activiteiten die mogelijk ook Nederlandse belangen kunnen schaden. Daarnaast is het mogelijk dat Nederlandse ICT-infrastructuur wordt misbruikt voor aanvallen elders. Als hackers aanvallen vanuit of via Nederland uitvoeren op buitenlandse doelwitten, kan Nederland getroffen worden door een tegenreactie.[35]

[35] Zie het Cybersecuritybeeld Nederland 2022: https://www.nctv.nl/onderwerpen/cybersecuritybeeld-nederland/documenten/publicaties/2022/07/04/cybersecuritybeeld-nederland-2022.

Dreigingscategorie 3: Statelijke politieke spionage

Onder deze dreigingscategorie vallen digitale aanvallen die, in de context van de oorlog, gericht zijn op het verkrijgen van vertrouwelijke gegevens. Nederlandse organisaties die gevoelige informatie van strategische aard bezitten, moeten nog steeds rekening houden met dit scenario.

Statelijke politieke spionage

In de huidige fase van de oorlog voert, naast beïnvloeding, digitale spionage de boventoon.[36] Een van de voornaamste doelstellingen van statelijke actoren is om, vaak via (spear)phishing, informatie te vergaren over politieke, bestuurlijke en/of diplomatieke ontwikkelingen ten aanzien van de oorlog in Oekraïne. De verkregen informatie dient het verbeteren van de informatiepositie om bijvoorbeeld voorkennis op te doen over politieke standpunten, de eigen onderhandelingspositie te versterken en besluitvorming te ondersteunen. Politieke organisaties of partijen in de vitale sector, die betrokken zijn bij gevoelige politiek-strategische thema's, kunnen het doelwit worden van dergelijke aanvallen.[37] In dreigingscategorie 5 wordt specifiek ingegaan op economische spionage.

Het NCSC heeft op 26 juli 2022 een analyse uitgebracht over deze dreigingscategorie ("Digitale spionageactiviteiten door statelijke actoren"). Het beeld dat deze analyse schetst is nog steeds van toepassing.

Een al langer bestaand probleem

Digitale spionageactiviteiten hoeven niet een directe relatie tot de oorlog in Oekraïne te hebben. Waargenomen campagnes passen in een breder patroon waarin statelijke actoren gerichte digitale spionageaanvallen uitvoeren op diplomatieke, publieke en politieke organisaties in Europa. Wel kunnen ontwikkelingen omtrent de oorlog en de

[36] https://www.ncsc.nl/onderwerpen/oekraine-aivd-mivd

[37] Zo meldde Microsoft op 22 juni 2022 dat het sinds de start van de oorlog pogingen tot spionage heeft gedetecteerd op 128 doelen in 42 landen buiten Oekraïne. 49% hiervan zijn overheidsinstellingen en 12% zijn ngo's (denktanks die adviseren over buitenlands beleid of humanitaire organisaties die hulp verlenen aan Oekraïense burgers). De overige 39% is gericht op IT-bedrijven (20%) en kritieke infrastructuur (19%).

verslechterde relatie tussen Rusland en het Westen een effect hebben op de omvang en intensiteit van deze activiteiten.[38]

		Waarschijnlijkheid per conflictstadium		
		Voortzetting van de oorlog	Staakt-het-vuren	Vredesovereenkomst
3	Digitale spionageactiviteiten door statelijke actoren	Waarschijnlijk —	Waarschijnlijk —	Waarschijnlijk —

Politieke spionagecampagnes op EU- en NAVO-leden

In de afgelopen maanden zijn door verschillende organisaties digitale spionageaanvallen van statelijke actoren waargenomen die, naast Oekraïne, primair gericht zijn op de publieke sector van NAVO- en EU-lidstaten.[39] Zo meldt Microsoft dat de Russische actor SEABORGIUM de Oekraïense overheid digitaal heeft aangevallen, met spionage als waarschijnlijk motief.[40] NAVO-lidstaten zijn volgens Microsoft het primaire doelwit van SEABORGIUM, waar deze actor het onder andere gemunt heeft op de defensie- en inlichtingensector, denktanks, hoger onderwijs, ngo's en intergouvernementele organisaties. De Russische actor Turla heeft eveneens een digitale spionagecampagne uitgevoerd, ditmaal op een elektronisch leerplatform van de NAVO, het Baltic Defence College en de Economische Kamer van Oostenrijk.[41] Ook hoogwaardigheidsbeklederslopen een verhoogd risico slachtoffer te worden van een spionageaanval, alsmede omringende staf met toegang tot relevante informatie zoals inhoudelijke dossiers, systemen en agenda's.[42]

Waargenomen digitale spionage-aanvallen zijn voornamelijk gericht op organisaties die betrokken zijn bij gevoelige politieke, militaire of economische besluitvorming.[43] E-

[38] https://www.mandiant.com/resources/tracking-apt29-phishing-campaigns

[39] Zie bijvoorbeeld https://unit42.paloaltonetworks.com/cloaked-ursa-online-storage-services-campaigns/ en https://www.mandiant.com/resources/tracking-apt29-phishing-campaigns.

[40] https://www.microsoft.com/en-us/security/blog/2022/08/15/disrupting-seaborgiums-ongoing-phishing-operations/

[41] https://blog.sekoia.io/turla-new-phishing-campaign-eastern-europe/

[42] Zo zouden Russische hackers berichten hebben weten te onderscheppen van Liz Truss, ex-premier van het VK. Zie voor meer informatie bijlage E.

[43] Zie bijvoorbeeld https://cert.gov.ua/article/39086, https://www.microsoft.com/security/blog/2021/05/27/new-sophisticated-email-based-attack-from-nobelium/,

mailaccounts en interne netwerken van deze organisaties kunnen een doelwit voor digitale spionageactiviteiten van statelijke actoren zijn. Het uitzetten van Russische diplomaten, die mogelijk politieke, economische en militaire informatie hebben verzameld in Nederland,[44] maakt Rusland mogelijk afhankelijker van digitale middelen om aan spionage te kunnen blijven doen. Het NCSC acht de kans van dit scenario daarom in het geval van Nederland **nog steeds waarschijnlijk** voor doelgroepen die zich met politiek-strategische doeleinden bezighouden. In de aanloop tot een mogelijk staakt-het-vuren of zelfs een eventuele vredesovereenkomst bestaat nog steeds een mogelijke intentie vanuit kwaadwillende actoren om een goede informatiepositie te behouden. Het NCSC verwacht daarom niet dat deze dreiging in de nabije toekomst zal afnemen.

https://unit42.paloaltonetworks.com/cloaked-ursa-online-storage-services-campaigns/ en https://www.mandiant.com/resources/tracking-apt29-phishing-campaigns.

[44] https://nos.nl/artikel/2448320-dit-weten-we-over-de-russische-spionnen-in-nederland

Dreigingscategorie 4: Aantasting van de informatievoorziening

Onder deze dreigingscategorie vallen digitale aanvallen die de informatievoorziening van Nederlandse organisaties treffen en tot doel hebben de publieke perceptie, maatschappelijke trends en/of politieke besluitvorming te beïnvloeden. In deze update is gekozen om ook defacement-aanvallen uit te lichten.[45] Waarschijnlijkheidsinschattingen in deze dreigingscategorie zijn grotendeels stabiel gebleven. Het is twijfelachtig of desinformatie via gecompromitteerde accounts, defacement-aanvallen en hack-en-lek operaties plaatsvinden in Nederland. In een nieuw scenario houdt het NCSC wel rekening met de mogelijkheid dat de informatievoorziening van overheidsinstanties verstoord raakt, met name door DDoS-aanvallen.

Het NCSC en desinformatie

Ondanks het belang dat Rusland hecht aan de inzet van beïnvloedingsmiddelen voor het behalen van strategische en tactische doelstellingen[46] [47], heeft de inzet op dit vlak waarschijnlijk niet het beoogde effect gehad.[48] Desalniettemin blijft waakzaamheid hieromtrent geboden, met name omdat Russische actoren snel kunnen inspelen op de actualiteit. Hierbij kunnen diverse aanvalstechnieken worden ingezet. Informatiecampagnes die ingaan op de ontwikkelingen op het slagveld zijn hierin een belangrijk component, maar niet het enige middel. In het verleden zijn bijvoorbeeld

[45] Een supply chain-aanval waar in eerdere publicaties nog specifiek op in werd gegaan, is hierin verwerkt als een mogelijke aanvalsvector. Ook zijn hack-en-lek operaties overgeplaatst naar deze categorie. Deze maakten in eerdere versies onderdeel uit van dreigingscategorie 3, maar passen in het bredere beeld van operaties die trachten de publieke perceptie te beïnvloeden. Tot slot zijn verstorende aanvallen op de informatievoorziening aan deze dreigingscategorie toegevoegd.

[46] Zie voor een gedetailleerd overzicht het boek "Active Measures – The Secret History of Disinformation and Political Warfare" van *Thomas Rid* waarin beïnvloedingscampagnes sinds het oprichten van Russische inlichtingendienst de Cheka (de voorloper van o.a. de KGB en de huidige I&V-diensten FSB en SVR) worden behandeld. Veel van de activiteiten die nu in het cyber domein plaatsvinden zijn digitale varianten van praktijken die sindsdien in uitvoer zijn gebracht.

[47] Zie voor meer inzicht in strategische doelstelling en uitvoer hiervan op tactisch niveau o.a. https://www.rand.org/pubs/research_reports/RRA704-1.html, https://isc.independent.gov.uk/wp-content/uploads/2021/03/CCS207_CCS0221966010-001_Russia-Report-v02-Web_Accessible.pdf & https://blogs.microsoft.com/on-the-issues/2022/06/22/defending-ukraine-early-lessons-from-the-cyber-war/.

[48] Zie bijvoorbeeld "https://www.bbc.com/news/world-europe-63272202 & https://www.wired.com/story/putin-collapse-disinformation-machinery-ukraine/

hack-en-lek aanvallen en aantasting van online beschikbare informatie ingezet op strategische momenten, waaronder verkiezingen in Oekraïne, maar ook bijvoorbeeld in de VS, het VK en Frankrijk.[49] Naarmate het conflict voortduurt, zullen zich meer mogelijkheden voordoen voor actoren om maatschappelijk vertrouwen en democratische processen te verstoren. De rol van hacktivisten valt hierin op, zowel als zelfstandig opererende actoren als groeperingen die een dekmantel vormen voor of samenwerken met statelijke actoren.

Evenals in eerdere publicaties kijkt het NCSC naar dit onderwerp met het oog op de integriteit en beschikbaarheid van informatiesystemen. Eventuele doelwitten van aanvallen binnen deze categorie kunnen mediabedrijven, publieke, politieke en/of maatschappelijk invloedrijke instanties en/of individuen zijn.[50] Beïnvloedingscampagnes middels nepaccounts op sociale media, botgestuurde tweets en andere heimelijke beïnvloedingspraktijken door actoren zoals de IRA (Internet Research Agency) worden hierin niet meegenomen.

		Waarschijnlijkheid per conflictstadium		
		Voortzetting van de oorlog	Staakt-het-vuren	Vredesovereenkomst
4A	Desinformatie via gecompromitteerde accounts	Twijfelachtig —	Twijfelachtig —	Twijfelachtig —
4B	Defacement-aanvallen en aantasting van online beschikbare informatie	Twijfelachtig —	Onwaarschijnlijk ↓	Onwaarschijnlijk —
4C	Hack-en-lek operaties met een politiek motief	Twijfelachtig ↓	Twijfelachtig —	Twijfelachtig —
4D	*Nieuw scenario:* Verstoring van informatievoorziening overheidsinstanties	Mogelijk	Twijfelachtig	Twijfelachtig

[49] Zie o.a. https://cyberlaw.ccdcoe.org/wiki/Ukrainian_parliamentary_election_interference_(2014); https://www.atlanticcouncil.org/in-depth-research-reports/report/the-macron-leaks-operation-a-post-mortem/; https://www.bbc.com/news/uk-politics-53433523 & https://www.justice.gov/file/1080281/download.

[50] https://www.oodaloop.com/archive/2021/12/22/c-suite-guide-to-improving-your-cybersecurity-posture-before-russia-invades-ukraine/

4A: Desinformatie via gecompromitteerde accounts

Desinformatie via gecompromitteerde accounts speelt een beperkte rol binnen het conflict. Hoewel dit relatief gemakkelijk uitgevoerd kan worden, wordt compromittatie vaak snel opgemerkt en is de impact vaak beperkt en van korte duur. Geplaatste berichten via een gecompromitteerd account worden met name gebruikt om desinformatie te verspreiden en bijvoorbeeld de legitimiteit van claims te onderbouwen. Zo werd recent nog het persoonlijke Instagram-account van de Commandant van de Oekraïense Krijgsmacht gehackt. Hierdoor kon de aanvaller onder andere een bericht plaatsen over de zogenaamde compromittatie van het DELTA-systeem dat gebruikt wordt voor het monitoren van het slagveld. Dit bericht werd daarna verder verspreid via andere kanalen.[51] Ook buiten Oekraïne kan dit een middel zijn om desinformatie legitimiteit te verschaffen. Het bericht dat de Poolse overheid betrokken was bij deportaties van Oekraïense vluchtelingen werd bijvoorbeeld schijnbaar onderbouwd via een social media-account van een Poolse politicus.[52] [53] Google TAG merkte in juli op dat Ghostwriter[54] zich ook richt op social media-accounts van Poolse burgers, waarbij gebruik wordt gemaakt van de phishing-techniek "browser in the browser".[55] [56] Ook compromittatie van nieuwsorganisaties om zodoende desinformatie te verspreiden, vallen hieronder.[57]

Voor specifieke politiek-strategische doelgroepen[58] in Nederland zijn dergelijke compromittaties tot op heden niet waargenomen. Het NCSC schat dit scenario daarom

[51] https://www.pravda.com.ua/eng/news/2022/11/3/7374847/

[52] https://www.cyberscoop.com/ghostwriter-disinformation-russia-belarus-poland-ukraine-refugees/

[53] https://www.wired.com/story/ghostwriter-hackers-belarus-russia-misinformationo/

[54] Mogelijk gelieerd aan de Wit-Russische overheid, zie https://www.mandiant.com/resources/blog/unc1151-linked-to-belarus-government

[55] Bij de "browser in the browser"-techniek vervalst de aanvaller een browservenster, binnen een ander venster, om zo inloggegevens te stelen. Zie voor meer informatie bijvoorbeeld https://medium.com/@Jscrambler/browser-in-the-browser-a-new-wave-of-picture-in-picture-phishing-attacks-39bc65080905.

[56] Dit sluit ook aan bij het beeld uit eerdere Ghostwriter-campagnes tussen 2017 en 2021, waarbij niet alleen social media media-accounts werden gehackt, maar waarbij ook desinformatie werd verspreid via gecompromitteerde legitieme nieuwssites. Zie https://blog.google/threat-analysis-group/continued-cyber-activity-in-eastern-europe-observed-by-tag/.

[57] Zie bijvoorbeeld https://www.cyberscoop.com/hackers-infiltrate-ukrainian-radio-network-broadcast-fake-message-about-zelenskys-health/

[58] Hieronder wordt verstaan doelgroepen die betrokken zijn in politieke, militaire en/of bestuurlijke besluitvorming en doelgroepen die een aanzienlijke rol hebben m.b.t. de publieke beeldvorming, zoals politieke organisaties, overheidsinstanties, denktanks en/of de media.

voor Nederland **nog steeds in als twijfelachtig.** Waarschijnlijk is dat een eventuele dergelijke compromittatie opportunistisch van aard zou zijn. Meer gerichte aanvallen die bijdragen aan tactische doelstellingen kunnen echter niet uitgesloten worden.

4B: Defacement-aanvallen gericht op het beïnvloeden van de publieke opinie

Zowel in Oekraïne als in Rusland heeft een groot aantal defacement-aanvallen plaatsgevonden. Hierbij wordt oneigenlijk toegang tot een website verkregen, waarna deze wordt beklad met bijvoorbeeld opruiende, verontrustende en provocerende teksten. Het startschot hiervoor werd gegeven in januari, toen tientallen overheidswebsites van Oekraïne middels een supply chain-aanval werden aangepast met een dreigend bericht gericht aan Oekraïense burgers.[59] Sindsdien zijn op grote schaal bekladdingen van websites uitgevoerd over en weer, waarbij zowel pro-Russische als pro-Oekraïense berichten worden gedeeld. Dergelijke aanvallen zijn relatief makkelijk uit te voeren en worden voor een groot deel uitgevoerd door niet-statelijke actoren. Het vergroten van de eigen reputatie speelt hierbij ook een rol.[60] Aanvallers die daadwerkelijk de publieke perceptie proberen te beïnvloeden richten zich met name op overheidswebsites en mediaorganisaties. Denk hierbij ook aan het onderbreken van uitzendingen op tv met alternatieve berichtgeving (ook wel *signal-hijacking* genoemd).[61]

Dergelijke aanvallen in de context van het conflict richten zich specifiek op de moraal van de betrokken partijen en/of de beeldvorming hieromtrent en passen daarom minder in de context van het Nederlandse debat waarin een pluriformiteit van meningen vertegenwoordigd is. Dat een dergelijke aanval zich specifiek zou richten op Nederland met als doel de publieke opinie te beïnvloeden, lijkt daarom **nog steeds twijfelachtig**. Bij verdere de-escalatie neemt de kans hierop verder af.

4C: Hack-en-lek operaties met een politiek motief

In de afgelopen maanden hebben zowel statelijke als niet-statelijke actoren diverse hack-en-lek aanvallen opgeëist. Zoals eerder aangegeven, ging dit in sommige gevallen samen met de inzet van wiperware. Deze aanvallen zijn uitgevoerd op zowel (Westerse)

[59] https://www.bleepingcomputer.com/news/security/russian-government-sites-hacked-in-supply-chain-attack/

[60] https://www.scmagazine.com/analysis/ransomware/third-party-hacking-groups-lose-interest-in-russia-ukraine-conflict-study-claims

[61] Zie bijvoorbeeld https://cip.gov.ua/en/news/kiberataka-rosiyi-na-servis-oll-tv

bedrijven als Oekraïense en Russische overheidsinstanties of daaraan gelieerde organisaties.[62] Dergelijke aanvallen hebben tot doel oneigenlijk verkregen vertrouwelijke informatie te publiceren om zo reputatieschade te veroorzaken bij het slachtoffer en/of een bredere maatschappelijke reactie te bewerkstelligen.[63] Hack-en-lek aanvallen kunnen verschillende vormen aannemen, waaronder het aanpassen van documenten, het achterhouden van informatie, het publiceren onder een valse naam en/of het vervalsen van de herkomst van gepubliceerde data. Dit is niet altijd noodzakelijk, bijvoorbeeld als gehackte bestanden voldoende informatie bevatten om het beoogde doel te behalen. Het onderscheid tussen wat echt is en wat nep, is vaak onduidelijk. Ook blijkt niet altijd duidelijk of gepubliceerde documenten daadwerkelijk bemachtigd zijn middels een digitale aanval of dat gelekte documenten überhaupt bestaan. Alleen al de claim dat dit het geval is, kan zorgen voor maatschappelijke onrust.[64]

De nadruk van dergelijke aanvallen en claims ligt op partijen die direct dan wel indirect een rol spelen in het conflict door bijvoorbeeld een (vermeende) bijdrage te leveren aan een van de twee strijdende partijen. Er bestaat wat dat betreft ook een intentie van hacktivisten om onder andere Westerse bedrijven onder druk te zetten. Het inschatten van de daadwerkelijke capaciteit die dergelijke groeperingen bezitten, blijft echter lastig. Dat het uitvoeren van een hack-en-lek aanval niet vanzelfsprekend is, blijkt uit het feit dat meerdere claims op dit vlak achteraf niet waar blijken te zijn.[65] Bij statelijke actoren is het omgekeerde het geval. Hoewel de capaciteit aanwezig is (blijkens eerder vernoemde hack-en-lek operaties), is de intentie diffuser. De focus lijkt momenteel in ieder geval niet op Nederlandse organisaties te liggen en wordt daarom **bijgesteld naar**

[62] Zie bijvoorbeeld https://www.infosecurity-magazine.com/news/russian-reservists-leaked-anonymous/ en https://www.vice.com/en/article/4ax459/pro-ukraine-hacktivists-claim-to-have-hacked-notorious-russian-mercenary-group

[63] Voorbeelden hiervan zijn hack-en-lek operaties op de overheid van Moldavië in 2022, het Europees Geneesmiddelenbureau in 2020, aanvallen op de Britse verkiezingen in 2019, aanvallen op de Franse verkiezingen in 2017 en de Amerikaanse verkiezingen in 2016.

[64] Zo verspreidde de pro-Russische hacktivistische groeperingen RaHDIt en Beregini valse geruchten over het bemachtigen van informatie over het aantal doden binnen het Oekraïense leger en over het terugsturen van Oekraïense vluchtelingen door de Poolse overheid. In het laatste geval werd een zogenaamd officieel overheidsdocument gelekt via Telegram als ondersteunend bewijs. Zie https://english.nv.ua/nation/russian-propagandists-spreading-fake-information-about-ukrainian-army-losses-50255674.html & https://www.cyberscoop.com/ghostwriter-disinformation-russia-belarus-poland-ukraine-refugees/

[65] Zie bijvoorbeeld https://fortune.com/2022/03/23/nestle-anonymous-leak-hack-russia-business-kitkat-nesquik/; https://www.newsweek.com/himars-maker-lockheed-martin-cyberattack-russian-hackers-1732504 & https://www.lemonde.fr/en/pixels/article/2022/11/12/thales-lockbit-releases-stolen-data-company-denies-any-intrusion-into-its-it-systems_6003921_13.html

twijfelachtig. Dit beeld kan wel veranderen. Bijvoorbeeld tijdens verkiezingen of andere belangrijke maatschappelijke debatten.

4D: Verstoring van informatievoorziening overheidsinstanties

Een recente ontwikkeling is de toenemende aandacht die uitgaat naar DDoS-aanvallen op websites van overheidsinstanties. Deze zijn niet alleen gericht op Russische en Oekraïense organisaties, maar voeren pro-Russische actoren ook uit op organisaties in de EU en de VS.[66] Hoewel deze aanvallen over het algemeen een beperkte en voornamelijk symbolische impact hebben, kunnen dergelijke aanvallen wel degelijk (tijdelijk) van invloed zijn op de informatieverstrekking en dienstverlening aan burgers. Ook kunnen deze incidenteel de politieke besluitvorming verstoren, zoals het geval was bij een digitale aanval op het parlement van Slowakije, waardoor stemmingen moesten worden uitgesteld.[67] Dergelijke aanvallen hebben een duidelijke politieke signatuur en worden veelal opgeëist door hacktivistische actoren. Ook de timing is hierbij opvallend omdat deze DDoS-aanvallen vaak worden ingezet naar aanleiding van politieke besluitvorming of gedane uitspraken. Zo werd recent een DDoS-aanval uitgevoerd op de website van het Europees Parlement na een stemming over het aanwijzen van Rusland als staatssponsor van terrorisme.[68] [69] Zwaardere aanvalsmiddelen gericht op Oekraïense overheidsinstanties, zoals de inzet van wipers, lijken met name in het begin van het conflict te zijn waargenomen.[70] Mogelijk hebben een sterk defensieve houding en internationale steun bijgedragen aan de relatief beperkte impact hiervan.[71]

---

[66] In reactie hierop werd in juli 2022 door de EU een verklaring aangenomen om DDoS-aanvallen tegen EU-lidstaten en partners te veroordelen, zie https://www.consilium.europa.eu/nl/press/press-releases/2022/07/19/declaration-by-the-high-representative-on-behalf-of-the-european-union-on-malicious-cyber-activities-conducted-by-hackers-and-hacker-groups-in-the-context-of-russia-s-aggression-against-ukraine/.

[67] https://www.reuters.com/world/europe/slovak-parliament-suspends-voting-due-suspected-cyberattack-2022-10-27/. Zie ook https://www.thelocal.se/20220911/swedish-election-authority-hit-by-three-cyber-attacks-around-election/.

[68] https://www.politico.eu/article/cyber-attack-european-parliament-website-after-russian-terrorism/

[69] KillNet claimde eerder onder andere een DDoS-aanval op de website van het Letse parlement nadat deze Rusland officieel had aangewezen als sponsor van terrorisme. Zie https://therecord.media/pro-kremlin-hackers-target-latvias-parliament-after-declaring-russia-a-sponsor-of-terrorism/

[70] Zie voor een overzicht https://www.cisa.gov/uscert/ncas/alerts/aa22-057a

[71] https://blogs.microsoft.com/on-the-issues/2022/06/22/defending-ukraine-early-lessons-from-the-cyber-war/

Een verstoring van de informatievoorziening in Nederland wordt **ingeschaald op mogelijk**. Hierbij moet wel in acht worden genomen dat in een dergelijk scenario wordt uitgegaan van een DDoS-aanval met beperkte impact. De inzet van andere verstorende middelen lijkt een stuk onwaarschijnlijker en zou een aanzienlijke escalatie betekenen van wat tot nu toe is waargenomen.[72] Dit past ook niet in het beeld van de huidige doelstellingen van Russische actoren.

[72] Denk hierbij niet alleen aan de inzet van wiperware, maar ook aan de gebruikte modus operandi tegen TV5 Monde. Zie voor meer informatie bijvoorbeeld https://www.bbc.com/news/technology-37590375

Dreigingscategorie 5: Statelijke economische spionage

Onder deze dreigingscategorie vallen gerichte digitale aanvallen om op oneigenlijke wijze essentiële technologie te verkrijgen. Deze dreigingscategorie is een gevolg van de geïsoleerde positie van Rusland na de invasie in Oekraïne. De waarschijnlijkheid van digitale economische spionage is vanwege onder andere het aanhouden van de oorlog, het uitzetten van Russische diplomaten en de waargenomen inzet van dekmantelbedrijven bijgesteld naar mogelijk. Het NCSC adviseert op de lange termijn waakzaamheid voor mogelijke economische spionage vanuit Rusland om technologische tekorten te compenseren.

Isolatie als mogelijke aanleiding voor digitale economische spionage

Zowel de westerse sancties als de bedrijven en technici die zijn weggetrokken naar aanleiding van de oorlog zorgen voor technologische tekorten in Rusland. In september 2022 meldt het Russische ministerie van Industrie en Handel dat Rusland te kampen heeft met een gebrek aan binnenlandse productiecapaciteit en dat het land onaantrekkelijk is geworden voor buitenlandse investeerders.[73] Het land heeft te kampen met een 'brain drain': grote aantallen technici zijn het land ontvlucht.[74] Ook hebben IT-leveranciers zich teruggetrokken en worden innovatie en productie lastiger, omdat essentiële onderdelen in toeleveringsketens moeilijker beschikbaar zijn.[75]

Het is bekend dat Russische inlichtingendiensten ook in Nederland actief op zoek zijn naar technologie.[76] Het NCSC houdt rekening met de mogelijkheid dat dit ook kan plaatsvinden door middel van digitale economische spionage.[77] Deze activiteiten kunnen met name gericht zijn op sectoren waar de EU sancties op heeft ingesteld, namelijk

[73] https://therecord.media/fears-grow-of-russian-spies-turning-to-industrial-espionage/

[74] https://apnews.com/article/russia-ukraine-putin-immigration-kazakhstan-technology-c041eb0b7472668087bb94207de2f71d

[75] https://www.bloomberg.com/news/articles/2022-06-28/russian-industry-faces-code-crisis-as-critical-software-pulled

[76] Zie het Dreigingsbeeld Statelijke Actoren 2: https://www.aivd.nl/documenten/publicaties/2022/11/28/dreigingsbeeld-statelijke-actoren-dbsa-2

[77] Ook internationale partners waarschuwen voor digitale economische spionage vanuit Rusland. Zo verwacht de Finse inlichtingen- en veiligheidsdienst SUPO de komende periode een toename in economische spionage te zien, omdat aanhoudende sancties de noodzaak voor Rusland verhogen om zelf hoogwaardige technologie te ontwikkelen: https://supo.fi/en/-/national-security-overview-russian-intelligence-changes-approach

financiën, handel, energie, vervoer, technologie en defensie.[78] Zo mogen bepaalde geavanceerde technologieën zoals kwantumcomputers en geavanceerde halfgeleiders, elektronica en software, maar ook technologieën in de energiesector, de zeescheepvaart en de lucht- en ruimtevaartindustrie niet uitgevoerd worden naar Rusland vanuit de EU.[79] Rusland ervaart hierdoor nu al tekorten en leveringsproblemen.[80]

		Waarschijnlijkheid per conflictstadium		
		Voortzetting van de oorlog	Staakt-het-vuren	Vredesovereenkomst
5	Statelijke economische spionage	Mogelijk ↑	Mogelijk —	Mogelijk —

Waargenomen fysieke activiteiten in Nederland

De MIVD meldt dat, om onder sancties uit te komen, de Russische militaire inlichtingendienst GRU dekmantelbedrijven opzet om technologieën in te kopen.[81] Dit betreft met name *dual-use* technologieën,[82] zoals producten voor de lucht- en ruimtevaart, microchips, kwantum- en nucleaire technologie en hightechelektronica. Sinds de start van de oorlog ziet de MIVD een toename in activiteit van deze dekmantelbedrijven,[83] wat duidt op een verhoogde Russische interesse in het verkrijgen van dergelijke technologieën.

Een ander voorbeeld hiervan is het Russische tekort aan chips. Uit onderzoek van de NOS blijkt dat enkele uitgezette Russische diplomaten geïnteresseerd waren in Nederlandse bedrijven die microchips ontwikkelen die gebruikt kunnen worden in de Russische wapenindustrie.[84] Ook heeft de Fiscale Inlichtingen- en Opsporingsdienst

[78] https://www.consilium.europa.eu/nl/policies/sanctions/restrictive-measures-against-russia-over-ukraine/

[79] https://www.consilium.europa.eu/nl/policies/sanctions/restrictive-measures-against-russia-over-ukraine/sanctions-against-russia-explained/

[80] https://www.ft.com/content/caf2cd3c-1f42-4e4a-b24b-c0ed803a6245

[81] https://fd.nl/economie/1454378/een-invasie-heeft-ook-grote-nadelige-gevolgen-voor-rusland-dat-ziet-poetin-ook-dachten-wij

[82] *Dual-use* technologieën kennen naast een civiele ook een militaire toepassing.

[83] https://fd.nl/economie/1454378/een-invasie-heeft-ook-grote-nadelige-gevolgen-voor-rusland-dat-ziet-poetin-ook-dachten-wij

[84] https://nos.nl/artikel/2448320-dit-weten-we-over-de-russische-spionnen-in-nederland

(FIOD) eind september 2022 een man in Nederland opgepakt, omdat hij onder andere microchips zou hebben geleverd aan Rusland.[85] [86]

Naast bovengenoemde fysieke activiteiten is het aannemelijk dat Rusland ook digitale middelen inzet om essentiële technologieën te verkrijgen.

Korte termijn: Directe behoefte aan eindproducten

Het is aannemelijk dat Russische actoren zich op de korte termijn richten op het (illegaal) inkopen/verkrijgen van eindproducten waar het land tekorten aan heeft. Actoren kunnen bijvoorbeeld trachten informatie te vergaren met betrekking tot gegevens, personen, bedrijven en procedures die een rol spelen bij de export van dergelijke producten. Hiervoor kan onder andere gebruik gemaakt worden van phishing-technieken of spoofing.[87]

Ook kleinere (keten)bedrijven en/of goederen die strategisch relevante componenten bevatten kunnen interessant zijn voor Russische statelijke actoren. Vergaarde inzichten kunnen bijdragen aan tactieken die ingezet worden om bijvoorbeeld exportrestricties te omzeilen.

Lange termijn: Ontwikkelen zelfstandigheid Russische industrie

Des te langer de economische isolatie van Rusland aanhoudt, des te meer dient men rekening te houden met een verhoogde dreiging van economische spionage. Op de langere termijn kan economische spionage zich meer richten op het oneigenlijk verkrijgen van technologie voor het ontwikkelen van de binnenlandse industrie. In het verleden hebben Russische actoren voor spionageactiviteiten onder andere gebruik gemaakt van technieken zoals (spear)phishing, HTML smuggling, DLL-sideloading en het installeren van backdoors,[88] alsmede supply chain- en watering hole-aanvallen om

[85] https://www.fiod.nl/aanhouding-in-onderzoek-naar-overtreding-sanctiewetgeving/

[86] De meeste chipfabrikanten, waaronder Intel, Samsung, TSMC en Qualcomm, hebben zich door de oorlog en internationale sancties teruggetrokken uit Rusland. Dit heeft geleid tot een tekort aan chips die worden gebruikt voor onder andere de productie van auto's, huishoudelijke apparaten en militaire doeleinden: https://www.ft.com/content/caf2cd3c-1f42-4e4a-b24b-c0ed803a6245

[87] Zie https://www.digitaltrustcenter.nl/informatie-advies/gehackt-wat-nu voor meer informatie over deze en andere gebruikte technieken.

[88] Zie voor meer informatie de publicatie van het NCSC over digitale spionageactiviteiten door statelijke actoren gepubliceerd in juli 2022. Neem contact op met het NCSC indien u dit document niet hebt ontvangen, maar wel zou willen inzien.

systemen te infecteren.[89] Deze technieken zijn ook geschikt om oneigenlijk toegang te verkrijgen tot gevoelige technologie.

Aangezien er nu al tekorten zijn ontstaan op de Russische markt en er geen aanwijzingen zijn voor een vredesovereenkomst waar een mogelijke normalisatie met het Westen aan is verbonden, stelt het NCSC de inschatting van dit scenario **omhoog bij naar mogelijk**. In april werd dit vanwege het zeer recent afkondigen van de sancties nog ingeschaald op twijfelachtig, omdat dit scenario met name op de langere termijn relevant is.

[89] Zie bijvoorbeeld https://attack.mitre.org/groups/G0035/

Dreigingscategorie 6: Digitale aanvallen voor financieel gewin

Deze dreigingscategorie betreft digitale aanvallen van niet-statelijke actoren met het oog op financieel gewin. De focus ligt hierbij op ransomware. Naast opportunistische aanvallen door niet-statelijke actoren, moet ook rekening gehouden worden met mogelijk politiekgekleurde ransomware-aanvallen. Zowel organisaties binnen de vitale sector als overheidsinstellingen kunnen hier slachtoffer van worden.

Veranderingen in het ransomware-landschap

In eerdere versies van de dreigingsscenario's is melding gemaakt van mogelijke samenwerkingsverbanden tussen statelijke en niet-statelijke actoren. Niet-statelijke actoren kunnen bijvoorbeeld worden aangemoedigd, of onder druk worden gezet, door statelijke actoren om verstorende operaties uit te voeren.[90] In de afgelopen periode is het opvallend dat een aantal impactvolle ransomware-aanvallen, door van oorsprong Russische criminelen, zijn uitgevoerd op overheden en/of overheidsinstanties die steun aan Oekraïne hebben uitgesproken. [91] Ook zijn er recent meerdere ransomware-aanvallen geweest die aan een statelijke actor worden toegekend.[92] Hoewel de relatie met statelijke actoren over het algemeen ambigu is en er onduidelijkheid kan bestaan over de achterliggende intentie van bepaalde ransomware-actoren, is de dreiging wel degelijk aanwezig.[93] Ook hier geldt dat weerbaarheid een belangrijke factor is voor mitigatie, aangezien doelwitselectie ook hier vaak grotendeels opportunistisch van aard is.

[90] Florian J. Egloff & Max Smeets (2021) "Publicly attributing cyber attacks: a framework", *Journal of Strategic Studies*.

[91] Let wel, het is goed mogelijk dat deze aanvallen zijn uitgevoerd met het oog op financieel gewin zonder enige vorm van statelijke druk. Mogelijk is ook dat bepaalde aanvallen kunnen bijdragen aan een goede verstandhouding met statelijke actoren, zonder dat deze als opdrachtgever fungeren.

[92] In scenario 1A werd al Prestige-ransomware genoemd. Ook de RansomBoggs-ransomware lijkt gerelateerd aan de statelijke actor Sandworm: https://www.welivesecurity.com/2022/11/28/ransomboggs-new-ransomware-ukraine/.

[93] Een ander voorbeeld hiervan is de ransomware-groep Yanluowang, waarvan er ook vermoedens bestaan dat ze nauwe banden onderhouden met Russische statelijke actoren: https://www.infosecurity-magazine.com/news/yanluowang-ransomwares-russian/

		Waarschijnlijkheid per conflictstadia		
		Voortzetting van de oorlog	Staakt-het-vuren	Vredesovereenkomst
6	Digitale aanvallen voor financieel gewin	Waarschijnlijk —	Waarschijnlijk —	Waarschijnlijk —

Politiekgekleurde ransomware-aanvallen?

Vlak na het begin van de oorlog in Oekraïne sprak de Conti-groep steun uit voor de Russische regering. Later stelt de groep echter niet aan de Russische overheid gelieerd te zijn.[94] In april 2022 compromitteerde Conti vervolgens diverse overheidsinstanties in Costa Rica. Opvallend is dat deze aanval plaatsvond tijdens de instelling van een nieuw kabinet in Costa Rica en dat de Costa Ricaanse president hiervoor steun voor Oekraïne uitsprak.[95] In diverse posts op de Conti-blog werd gesteld dat er geen sprake is van inmenging van overheden in deze aanval, hoewel er wel kritiek werd geuit op de relatie tussen de VS en Costa Rica.[96] Naast de losgeldeis riep Conti op tot publieke onrust in Costa Rica om de regering daar verder onder druk te zetten.[97] De oproep tot maatschappelijke onrust door een ransomware-groep is nieuw en niet eerder waargenomen door het NCSC. Costa Rica is ook niet het enige overheidsslachtoffer van Conti. Vlak na de aanval op Costa Rica werd namelijk ook een grote hoeveelheid data van de Peruviaanse veiligheidsdienst op Conti's leakblog gepost.[98] [99]

[94] https://www.reuters.com/technology/russia-based-ransomware-group-conti-issues-warning-kremlin-foes-2022-02-25/

[95] https://www.ukrinform.net/rubric-polytics/3534202-zelensky-thanks-costa-rica-president-for-supporting-ukraine-in-international-organizations.html

[96] https://www.cyberscoop.com/conti-costa-rica-ransomware-peru-unc1756/

[97] Zie https://apnews.com/article/technology-government-and-politics-caribbean-gangs-381efc2320abb5356dee7f356e55e608; https://www.nacion.com/el-pais/servicios/funcionarios-del-ice-evaluaran-ciberseguridad-de/I4S3BCQ6MRFTTIFOIN7S5YVBHY/story/; https://www.crhoy.com/tecnologia/a-un-mes-del-inicio-de-ciberataques-estas-son-las-consecuencias-sin-solucion/; & https://www.bbc.com/mundo/noticias-america-latina-61516874

[98] https://www.cyberscoop.com/conti-costa-rica-ransomware-peru-unc1756/

[99] Eind mei werd de Conti-operatie opgedoekt. Volgens Intel471 begonnen in mei 2022 aan Conti gelieerde actoren naar verluidt samen te werken met andere ransomware-operaties, zoals BlackCat en Hive. De Hive ransomware-aanval op Costa Rica en een ransomware-aanval op een technologiebedrijf dat eerder door Conti was geraakt onderstreept dit vermoeden.

In augustus dit jaar werd ook Montenegro slachtoffer van een ransomware-aanval. Eind augustus claimde de Montenegrijnse veiligheidsdienst dat het om een gecoördineerde Russische aanval gaat, de term hybride oorlog valt hier ook.[100] Het Russische ministerie van Buitenlandse Zaken ontkende enige betrokkenheid via Twitter.[101] Een aantal dagen later volgde het bericht dat het gaat om een ransomware-aanval door de Cuba ransomware-groep.[102] Opmerkelijk is dat CERT-UA naar aanleiding van een cyberaanval in oktober gericht op Oekraïense overheidsinstanties met RomCom-malware een mogelijke link met de actor UNC2596 ziet, die volgens CERT-UA mogelijk ook achter de Cuba ransomware-variant zit.[103] Recentelijk maakte ook ESET melding van de inzet van RansomBoggs-ransomware, mogelijk door de Russische statelijke actor Sandworm, tegen Oekraïense organisaties.[104]

Mogelijk veranderd dreigingslandschap voor overheden/overheidsinstanties

De waarschijnlijkheidsinschattingen voor dit scenario **blijven gehandhaafd op het niveau waarschijnlijk**. Hierbij moet wel gesteld worden dat in eerdere versies van dit document met name werd uitgegaan van ransomware-aanvallen voor financieel gewin op basis van een verminderende intentie vanuit Russische overheidsinstanties om in te grijpen. Hoewel dit onverminderd het geval is, komen mogelijk politiekgekleurde aanvallen met ransomware of wiperware daar bovenop. Deze dreiging geldt zowel voor organisaties binnen de vitale sector als voor overheidsinstellingen. In beide gevallen kan een dergelijke digitale aanval ook een psychologisch effect teweegbrengen en maatschappelijke impact hebben. Zoals eerder gesteld speelt de weerbaarheid van een organisaties een belangrijke rol als het aankomt op doelwitselectie.

[100] https://apnews.com/article/russia-ukraine-nato-technology-montenegro-adriatic-sea-54e93b841f737ec8bfdd4a9614869a8b

[101] https://mobile.twitter.com/mfa_russia/status/1564887688536375297

[102] https://www.bleepingcomputer.com/news/security/montenegro-hit-by-ransomware-attack-hackers-demand-10-million/

[103] Zie https://cert.gov.ua/article/2394117. Uit navraag bij Mandiant blijkt dat zij deze malware, die zij volgen onder een andere naam, ook in combinatie zien met andere ransomware-varianten en dat deze malware dus niet exclusief gebruikt wordt door Cuba-groep.

[104] https://www.welivesecurity.com/2022/11/28/ransomboggs-new-ransomware-ukraine/

Naast bovengenoemde ransomware-aanvallen zijn ook andere financieel-gemotiveerde aanvallen waargenomen. In een vorige update van dit document werden cryptominers reeds genoemd. Dit geldt ook voor phishingcampagnes met financieel motief.[105]

[105] Zo maakt Finland bijvoorbeeld melding van een verhoogd aantal phishingcampagnes door criminele actoren: https://www.traficom.fi/en/news/threat-level-cyber-environment-has-risen-activity-towards-finland-has-increased

Bijlage A: Achtergrond

Reikwijdte en toepassing

Reikwijdte

- Deze analyse is gericht op het in kaart brengen van het **dreigingslandschap** ten aanzien van de oorlog in Oekraïne voor Nederlandse overheidsorganisaties en vitale sectoren.
- In de analyse is beschikbare informatie tot **30 november 2022** gebruikt. Nieuwe ontwikkelingen kunnen een ander dreigingsbeeld geven.
- Het dreigingslandschap ten aanzien van de oorlog in Oekraïne is volatiel, complex en divers. Ontwikkelingen in de oorlog volgen elkaar snel op. Hierdoor zit er een aanzienlijke **onzekerheidsmarge** in de inschattingen van het NCSC.

Toepassing

- Deze analyse kan u **handvatten** geven **om de weerbaarheid van uw organisatie te verhogen** ten aanzien van digitale aanvallen die kunnen voortvloeien uit de oorlog in Oekraïne. Het NCSC gaat hierover graag met uw sector en/of organisatie in gesprek.
- Deze analyse is **geen risicoanalyse**. Het NCSC heeft de **weerbaarheid** van Nederlandse organisaties en sectoren niet meegenomen in de afwegingen.[106] De **impact** van een eventuele digitale aanval is zodoende ook **niet meegenomen** in de afwegingen.

Deze publicatie is **niet bedoeld voor andere doeleinden** dan om de Rijksoverheid en vitale aanbieders richting te geven bij het inzichtelijk maken van het digitale dreigingslandschap ten aanzien van de oorlog in Oekraïne **voor Nederland en Nederlandse organisaties**. Dit is een **specifieke vraagstelling** en daarom kunnen de uitkomsten van deze analyse op punten afwijken van analyses van andere veiligheidsorganisaties.

[106] Een verhoogde dreiging ten aanzien van een specifiek scenario hoeft niet te resulteren in daadwerkelijke effecten indien de weerbaarheid adequaat is.

Het scenarioraamwerk

Het NCSC maakt gebruik van zes dreigingscategorieën om digitale aanvallen te categoriseren die plaats kunnen vinden in de context van de huidige oorlog in Oekraïne en mogelijk impact kunnen hebben op de digitale veiligheid van Nederland. Deze zijn niet verder aangepast sinds de laatste publicatie van 28 april.

Conflictstadia

In de publicatie van 28 april is uitgebreid ingegaan op de verschillende stadia die een rol spelen binnen de escalatie en de-escalatie curve van een conflict. Deze analyse houdt hier aan vast en blijft bij de drie conflictstadia die toen zijn geïdentificeerd en die het verdere verloop van de oorlog in Oekraïne waarschijnlijk zullen kenmerken, te weten: (1) oorlog, (2) staakt-het-vuren en (3) vredesovereenkomst. Hierin houdt het NCSC rekening met een mogelijke de-escalatie van het conflict en met een verstoorde relatie tussen Rusland en het Westen, ook in de loop van 2023.

Waarschijnlijkheid

Het NCSC hanteert de volgende waarschijnlijkheidsinschattingen op basis van de intenties, capaciteiten en activiteiten van kwaadwillende actoren:

Onwaarschijnlijk	Twijfelachtig	Mogelijk	Waarschijnlijk	Zeer Waarschijnlijk	Bevestigd
Het is onwaarschijnlijk dat dit scenario zich gaat manifesteren in Nederland op korte termijn. *Actoren hebben niet de intentie dan wel capaciteit om over te gaan op een digitale aanval.*	Op basis van het huidige beeld is het twijfelachtig dat dit scenario in Nederland gaat plaatsvinden maar het zou in een uitzonderlijk geval kunnen. *Actoren kunnen (deels) de intentie of capaciteit bezitten om een digitale aanval uit te voeren.*	Het is mogelijk dat dit scenario gaat plaatsvinden en dat daarbij Nederlandse belangen in het geding komen. *Er is een verhoogde intentie van actoren met adequate capaciteit om het scenario uit te voeren.*	Het is waarschijnlijk dat dit scenario zich kan gaan manifesteren met eventuele gevolgen/ impact voor Nederland. *Actoren hebben een intentie en capaciteit om tot een digitale aanval over te gaan passend binnen strategische doelstellingen.*	Het is zeer waarschijnlijk dat dit scenario gaat gebeuren met gevolgen/ impact voor Nederland. *Er is een duidelijke intentie vanuit actoren met een bevestigde capaciteit om een digitale aanval uit te voeren.*	Het scenario is bevestigd. Deze situatie doet zich voor of gaat zich zeker in voordoen. *De actoren in kwestie hebben een bevestigde capaciteit en intentie om de aanval uit te voeren.*

Bijlage B: Handelingsperspectief

Een dreigingsanalyse als bouwsteen voor risicomanagement

Afhankelijk van uw organisatie zijn sommige dreigingen wellicht relevanter dan andere. Deze publicatie dient ervoor om de Nederlandse Rijksoverheid en organisaties in vitale sectoren handvatten te geven om zelfstandige dreigingsanalyses uit te voeren. Een dreigingsanalyse vormt samen met een belangen- en weerbaarheidsanalyse van uw organisatie de bouwstenen voor risicomanagement. Het NCSC kan helpen met het digitale risicomanagement van uw organisatie door te adviseren op de inrichting daarvan en door ondersteuning te bieden bij verschillende analyses.[107]

Eerdere publicaties

Verschillende publicaties kunnen u van handelingsperspectief voorzien tegen bekende modus operandi van betrokken actoren in de oorlog in Oekraïne:

- Zie voor het algemene handelingsperspectief met betrekking tot de scenario's de publicatie van 17 februari 2022 of de website van het NCSC.[108]
- Publicatie "Cyberaanvallen door statelijke actoren" van de AIVD en MIVD.[109]
- Analyse "Digitale spionageactiviteiten door statelijke actoren" van het NCSC.[110]
- Analyse "Hacktivistische activiteiten tijdens de oorlog in Oekraïne" van het NCSC.[111]

[107] https://www.ncsc.nl/documenten/brochures/2021/november/9/risicobeheersing

[108] https://www.ncsc.nl/onderwerpen/oekraine

[109] https://www.aivd.nl/documenten/publicaties/2021/06/28/cyberaanvallen-door-statelijke-actoren---zeven-momenten-om-een-aanval-te-stoppen

[110] Zie hiervoor de publicatie "Digitale spionageactiviteiten door statelijke actoren" van 26 juli 2022 van het NCSC.

[111] Zie hiervoor de publicatie "Hacktivistische activiteiten tijdens de oorlog in Oekraïne" van 8 september 2022 van het NCSC.

- Factsheet "Risico's beheersen: de waarde van informatie als uitgangspunt" van het NCSC.[112]

Neem contact op met het NCSC indien u verdachte digitale activiteiten waarneemt die mogelijk te herleiden zijn naar de oorlog in Oekraïne.

Het NCSC kan u helpen deze activiteiten te duiden en u te ondersteunen bij een eventueel incident. Het tijdig melden van incidenten bij het NCSC is in het belang van de Nederlandse digitale veiligheid. Uw input is van grote waarde voor ons situationeel beeld en de bescherming van Nederland.

Deelname aan het Nationaal Detectie Netwerk (NDN) helpt om op basis van technische details uw detectiemogelijkheden te vergroten.

[112] https://www.ncsc.nl/documenten/publicaties/2020/juli/21/factsheet-risicobeheersing

Bijlage C: Vervolgstappen naar aanleiding van TTP's

Het MITRE ATT&CK-raamwerk stelt u in staat mogelijke digitale aanvalstechnieken te identificeren en prioriteren om vervolgens daartegen maatregelen te treffen. Het NCSC heeft hier eerder in het jaar een blog over gepubliceerd. [113] Dit is een mogelijk aanknopingspunt voor een vertaalslag van deze scenario's naar operationeel en technisch niveau.

Het NCSC heeft hieronder een selectie gemaakt van relevante actoren en van gebruikte software waarmee een analyse gemaakt kan worden van veelvoorkomende TTP's, oftewel:

- Tactieken: technische doelstellingen (bijvoorbeeld het verkrijgen van toegang)
- Technieken: de wijze waarop een doelstelling wordt behaald (bijvoorbeeld spearphishing)
- Procedure: de specifieke implementatie van een techniek

TTP's kunnen gebruikt worden om inzicht te krijgen in de methodes die aanvallers hanteren. Op basis van deze methodes (in combinatie met een dreigingsinschatting voor uw specifieke organisatie) kan een verdedigings- en detectiestrategie worden ontwikkeld. Zo kunnen op basis van de gebruikte technieken en procedures specifieke mitigerende maatregelen worden toegepast en detectiemaatregelen genomen worden.

Een van de voordelen van het MITRE ATT&CK-raamwerk is dat het een uniforme beschrijving en benaming geeft van gehanteerde aanvalsmethodes. Daar komt bij dat het voor aanvallers vaak lastig is om hun gehanteerde TTP's te veranderen, waardoor deze voor een langere tijd bij kunnen dragen aan een verdedigingsstrategie.

De onderstaande lijst vormt een startpunt voor verdere analyse en is niet een compleet overzicht van betrokken actoren. Werkwijzen van andere actoren kunnen afwijken. Daarnaast kunnen gebruikte aanvalstechnieken aangepast worden om detectie te voorkomen.

[113] Zie voor meer informatie de blogpost van het NCSC over het gebruik van TTP's, https://www.ncsc.nl/actueel/weblog/weblog/2022/digitale-aanvalstechnieken-leer-je-tegenstander-kennen

Russische statelijke actoren

- APT28: https://attack.mitre.org/groups/G0007/
- APT29: https://attack.mitre.org/groups/G0016/
- Turla: https://attack.mitre.org/groups/G0010/
- Sandworm: https://attack.mitre.org/groups/G0034/
- UNC2589[114]: https://attack.mitre.org/groups/G1003/
- Gamaredon[115]: https://attack.mitre.org/groups/G0047/
- Dragonfly: https://attack.mitre.org/groups/G0035/

Actoren actief op het gebied van operationele technologie

Zie hiervoor o.a. de classificatie van Dragos met betrekking tot actoren en toegepaste TTP's binnen het OT-landschap: https://www.dragos.com/mitre-attack-for-ics/.

Relevante actoren zijn onder andere:

- ELECTRUM en KAMACITE (overlap met Sandworm)
- PETROVITE (overlap met APT28)
- XENOTIME (gelieerd aan de TRISIS/Triton malware)
- DYMALLOY (mogelijke relatie met Dragonfly)
- CHERNOVITE (gelieerd aan PIPEDREAM, ook wel INCONTROLLER, een aanvalsraamwerk gericht op ontwrichting en sabotage binnen OT-systemen waarvan het bestaan in april 2022 werd onthuld. Het vermoeden is dat het hier een statelijke actor betreft, volgens Mandiant mogelijk Russisch.[116] De tools zijn echter uniek en kunnen niet gelinkt worden aan een bestaande actor.)

Niet-statelijke actoren (crimineel)

- Conti: https://attack.mitre.org/software/S0575/. Hoewel Conti ransomware-as-a-service niet langer actief is, zijn diverse aan Conti gelieerde actoren wel actief in andere RaaS zoals onder meer ALPHV/BlackCat en Hive RaaS. Deze TTP's hebben daarom ook overlap met andere ransomware-aanvallen.
- Cuba: https://attack.mitre.org/software/S0625/

[114] UNC2589, of Ember Bear, is volgens MITRE ATT&CK een vermoedelijk door de Russische staat gesponsorde actor, zie https://attack.mitre.org/groups/G1003/. Deze actor richt zich met name op Oekraïne, maar is ook actief geweest tegen NAVO-lidstaten, zie https://www.mandiant.com/resources/blog/spear-phish-ukrainian-entities.

[115] Volgens Mandiant richt Gamaredon zich met name op Oekraïense doelen, hoewel aanvallen op Europese en Amerikaanse doelen ook zijn waargenomen. In het verleden is vaker gebleken dat Russische APT's buiten hun geografische focus treden. Daarom zijn TTP's van deze actor eveneens van belang.

[116] https://www.mandiant.com/resources/blog/incontroller-state-sponsored-ics-tool

Bijlage D: Precedentenonderzoek

Voor het precedentenonderzoek van digitale aanvallen in de context van een internationaal conflict verwijzen wij naar de publicatie van 17 februari 2022 en 28 april 2022. Dit onderzoek is gebaseerd op de beschikbare informatie voorafgaande aan de Russische invasie in Oekraïne.

Beschikt u niet over dit precedentenonderzoek, maar zou u dit wel willen inzien? Neem dan contact op met het NCSC.

Bijlage E: Ontwikkelingen

Tijdlijn digitale aanvallen

De volgende tijdlijn is een samenvatting van waargenomen digitale aanvallen die een (mogelijk) verband hebben met de oorlog in Oekraïne. De lijst is niet compleet. Het NCSC heeft een selectie gemaakt van incidenten om een algeheel beeld te schetsen van de diversiteit en intensiteit van de aanvallen. Een selectie van digitale aanvallen die hebben plaatsgevonden in de periode januari-april 2022 is te vinden in de publicatie van 28 april.

Dreigingscategorie 1: Doelgerichte digitale aanvallen gericht op sabotage van vitale infrastructuur

Datum	Aanval	Dreigings-categorie
3 mei	Google TAG neemt vaker actoren in het conflict waar die zich richten op het digitaal aanvallen van kritieke infrastructuur, waaronder olie en gas, telecommunicatie en productie. [🔒]	1
22 juni	Microsoft stelt dat het sinds de start van de oorlog acht verschillende malwareprogramma's, zowel wipers als andere vormen van destructieve malware, tegen 48 verschillende Oekraïense agentschappen en bedrijven heeft waargenomen. [🔒]	1
22 juni	Nadat Litouwen een verbod heeft ingesteld op doorvoer per spoor van Russische goederen naar Kaliningrad, roepen verschillende hacktivistische groeperingen op om vitale infrastructuur in Litouwen digitaal aan te vallen. [🔒]	1A, 2C

24 juni	CERT-UA waarschuwt voor digitale aanvallen op telecombedrijven in Oekraïne, waarbij gebruik wordt gemaakt van e-mails met een malafide bijlage. [🔒]	1B
30 juni	De Oekraïense overheidsinstantie SSSCIP meldt dat de intensiteit van digitale aanvallen op Oekraïne niet is afgenomen. Er hebben sinds de begin van de oorlog bijna 800 digitale aanvallen plaatsgevonden (Oekraïense overheid, lokale autoriteiten, defensie, energieleveranciers, financiële instanties). [🔒]	1, 3, 4
11 oktober	Microsoft neemt een ransomware/wiperware-campagne waar tegen transport en logistieke organisaties in Oekraïne. De ransomware wordt "Prestige"-ransomware genoemd. De activiteit heeft overeenkomsten met aan de Russische staat gerelateerde activiteit. [🔒]	1A, 6
24 oktober	De premier van Noorwegen waarschuwt dat Rusland "een reële en ernstige bedreiging" vormt voor de olie- en gasindustrie van het land. De premier stelt dat zijn land traag is met het nemen van de nodige maatregelen om kritieke infrastructuur in de energiesector te beschermen tegen cyberaanvallen. [🔒]	1C
25 november	RTL maakt melding van mogelijke interesse van Russische actoren in LNG-terminals in Nederland, op basis van informatie van cyberbeveiligingsbedrijf Dragos. [🔒]	1C

Dreigingscategorie 2: Spillover-effecten

Datum	**Aanval**	**Dreigings-categorie**
3 mei	APT Curious Gorge (China) wordt door Google TAG waargenomen als aanvaller van Oekraïense, Russische en Centraal-Aziatische (overheids)instanties. [🔒]	2B, 3
3 mei	Google TAG meldt dat financieel-gemotiveerde actoren de oorlog als thema gebruiken voor bijvoorbeeld malafide mails en linkjes. [🔒]	2B, 6
15 mei	DDoS-aanvallen gedurende de stemmingsronde van het Eurovisie Songfestival zijn volgens de Italiaanse politie gemitigeerd. [🔒] Deze aanvallen worden toegeschreven aan Killnet. [🔒]	2C
19 mei	Killnet voert aanvallen uit op ongeveer 50 Italiaanse organisaties, waaronder overheidsinstanties. Onder andere de websites van het Italiaanse ministerie van Buitenlandse Zaken en die van ambassades zijn onbereikbaar. [🔒]	2C, 4D

13 juni	Anonymous claimt een Russische dronefabrikant te hebben gehackt en zegt over Russische tactieken en plannen in de oorlog te beschikken. [🔓]	2C, 3, 4C
14 juni	De Wit-Russische hacktivistische actor Belarusian Cyber Partisans claimt toegang te hebben tot getapte gesprekken van onder andere de Russische ambassade in Wit-Rusland. Het zou gaan om opnames tussen 2020 en 2021. [🔓]	2C, 4C
22 juni	Nadat Litouwen een verbod heeft ingesteld op doorvoer per spoor van Russische goederen naar Kaliningrad, roepen verschillende hacktivistische groeperingen op om vitale infrastructuur in Litouwen digitaal aan te vallen. [🔓]	1A, 2C
22 juni	CERT-UA waarschuwt voor aan China gelieerde actoren die gebruik maken van digitale aanvallen tegen Russische organisaties. De aanvallers maken gebruik van phishing-emails met een malafide bijlage. Gebruikersinteractie met de bijlage resulteert in de installatie van Bisonal-malware waar spionage mee uitgevoerd kan worden. [🔓] [🔓]	2A, 3
29 juni	Killnet claimt DDoS-aanvallen te hebben uitgevoerd op diverse Noorse organisaties. [🔓]	2C
6 juli	Het Letse Radio en Televisie Center LVRTC is langdurig getroffen door een DDoS-aanval. Om de impact van de digitale aanval te beperken, heeft LVRTC de toegang tot bepaalde diensten tijdelijk uitgeschakeld. [🔓]	2C
7 juli	APT Tonto Team (China) richt zich op aan Rusland gelieerde organisaties met malware die is ontworpen om overheidsinformatie te stelen. [🔓]	2A, 3
27 juli	CERT-UA waarschuwt voor phishing-mails, zogenaamd afkomstig van het Rode Kruis, waarin om donaties wordt gevraagd voor Oekraïense vluchtelingen. De berichten bevatten een linkje naar een phishing-site die een Oekraïense bank nabootst. Inloggegevens die op deze site worden ingevuld, belanden in de handen van de aanvallers. [🔓]	2A, 6
4 augustus	Volgens Intel471 creëren leden van diverse pro-Russische hacktivistische groeperingen (Red Hackers Alliance Russia, Anonymous Russia, DeaDNet, Attacknet, NBP Hackers, the Rage Select, Aifaby, Fr13ndsNetw0rk) de Russian Cybersecurity Union om hun krachten te bundelen. Op 29 september claimt de beheerder van het KillNet Telegram-kanaal dat 14 Russische hackersgroepen,	2C

	waaronder Anonymous Russia, nu verenigd zijn onder de KillNet-paraplu.	
9 augustus	De website van het Finse parlement is getroffen door een DDoS-aanval. [🔒] De pro-Russische hackersgroep NoName057(16) zegt achter de aanval te zitten.	2C, 4D
11 augustus	Een DDoS-aanval vindt plaats op het Letse parlement. De digitale aanval gebeurde na het aannemen van een Letse verklaring die Rusland tot staatssponsor van terrorisme aanwijst. [🔒]	2C, 4D
13 augustus	Killnet zegt een DDoS-aanval te hebben uitgevoerd op defensieconcern Lockheed Martin. De groep zou ook persoonlijke gegevens hebben gestolen van medewerkers en dreigt deze gegevens te publiceren. [🔒]	2C, 4C
16 augustus	Het Oekraïense nucleaire agentschap Energoatom maakt melding van een Russische cyberaanval tegen zijn website. Volgens het agentschap zette de hackersgroep People's Cyber Army 7,25 miljoen bots in om de website onbereikbaar te maken. Volgens Energoatom heeft de aanval geen impact gehad op de werking van de site. [🔒]	2C
18 augustus	Estland slaat een grote DDoS-aanval af nadat het land een aantal Sovjet-monumenten heeft verwijderd. Deze aanvallen zouden zijn uitgevoerd door Killnet. [🔒]	2C
2 september	Anonymous beweert de grootste taxi service in Rusland, Yandex Taxi, te hebben gehackt. Door taxi's naar dezelfde locatie te sturen ontstonden diverse files in Moskou. [🔒]	2C
5 oktober	Killnet claimt een aantal Amerikaanse overheidswebsites offline te hebben gehaald. Het betreft websites van de staten Colorado, Mississippi en Kentucky. De meeste getroffen websites waren op dezelfde dag weer online. [🔒]	2C, 4D
10 oktober	Websites van Amerikaanse luchthavens, waaronder die van Atlanta (ATL), Los Angeles (LAX), Chicago (ORD) en Orlando (MCO), zijn getroffen door DDoS-aanvallen. Daardoor waren de websites tijdelijk ontoegankelijk. De aanvallen worden toegekend aan Killnet. De aanvallen zouden geen effect hebben gehad op vluchten van en naar de luchthavens. [🔒]	2C
15 oktober	Pro-Russische hackers voeren DDoS-aanvallen uit op Bulgaarse (overheids)organisaties. Deze veroorzaakten kleine storingen, maar de schade bleef volgens de Bulgaarse overheid beperkt. Killnet zegt verantwoordelijk te zijn. [🔒]	2C, 4D
14 november	Killnet claimt een DDoS-aanval op de website van de Amerikaanse FBI. [🔒]	2C, 4D

Dreigingscategorie 3: Statelijke politieke spionage

Datum	Aanval	Dreigings-categorie
23 mei	Onderzoekers van beveiligingsbedrijf Sekoia nemen digitale verkenningsactiviteiten waar van de Russische actor Turla. De activiteiten zijn gericht op de Baltic Defence College, de Economische Kamer van Oostenrijk en NAVO's eLearning platform genaamd JADL. De Economische Kamer van Oostenrijk is betrokken bij de uitvoering van sancties tegen Rusland. [🔗]	3
22 juni	Microsoft meldt dat het sinds de start van de oorlog pogingen tot spionage heeft gedetecteerd op 128 doelen in 42 landen buiten Oekraïne. 49% hiervan zijn overheidsinstellingen en 12% zijn ngo's (denktanks die adviseren over buitenlands beleid of humanitaire organisaties die hulpverlenen aan Oekraïense burgers). De overige 39% is gericht op IT-bedrijven (20%) en kritieke infrastructuur (19%). [🔗]	3, 5
15 juli	Volgens Symantec heeft de Russische APT Gamaredon tussen 15 juli en 8 augustus digitale aanvallen met Infostealer-malware uitgevoerd op Oekraïense organisaties. [🔗]	3
19 juli	Unit42 van Palo Alto waarschuwt voor (spear)phishing-aanvallen van APT29. De actor maakt hierbij gebruik van online storage-diensten zoals Dropbox en Google Drive. [🔗]	3
25 juli	Mandiant waarschuwt voor spearfishing-campagnes gelieerd aan de Russische actor UNC2589. De actor gebruikt sinds januari 2022 spearphishing-emails om de DARKTACO downloader, alsmede de CHEESEMELT en ASYNCRAT backdoors, te installeren. UNC2589 richt zich hierbij op doelwitten binnen Hongarije, Slowakije, Zwitserland en Oekraïne.	3
augustus	Volgens ESET maakt SaintBear/UNC2589 sinds juli gebruik van Cobalt Strike. Phishing-campagnes worden opgezet voor data exfiltratie of initial access.	3
15 augustus	Microsoft maakt melding van phishing-aanvallen van de Russische hackersgroep SEABORGIUM. De groep richt zich voornamelijk op NAVO-landen, Scandinavië en Oost-Europa, waaronder Oekraïne. De oorlog in Oekraïne wordt door deze groep ook gebruikt als onderwerp voor phishing-mails. [🔗]	3
29 oktober	Russische hackers zouden van september 2021 tot en met september 2022 berichten hebben weten te onderscheppen van Liz	3

	Truss, de ex-premier van het Verenigd Koninkrijk, met naar verluidt gevoelige informatie over de oorlog in Oekraïne. Volgens *The Mail on Sunday* bestonden de berichten ook uit gedetailleerde discussies over wapenleveringen. [🔒]	
11 november	Op 11 november 2022 heeft CERT-UA bericht over een hacktivistische campagne die zij toeschrijven aan de groepering From Russia with Love (FRwL). Bij deze campagne wordt een variant van Somnia-ransomware ingezet, waarbij er geen mogelijkheid zou zijn om de data te ontsleutelen. Het doel van deze campagne is niet financieel gewin, maar verstoring. [🔒] *Voor meer specifieke informatie over deze campagne en Indicators of Compromise, zie: https://cert.gov.ua/article/2724253.*	1, 3C, 6

Dreigingscategorie 4: Aantasting van de informatievoorziening

Datum	**Aanval**	**Dreigings-categorie**
9 mei	Russische satelliettelevisie toont pro-Oekraïense slogans, net voor de parade op Victory Day in Rusland. [🔒]	4B
19 mei	Killnet voert aanvallen uit op ongeveer 50 Italiaanse organisaties, waaronder overheidsinstanties. Onder andere de websites van het Italiaanse ministerie van Buitenlandse Zaken en die van ambassades zijn onbereikbaar. [🔒]	2C, 4D
5 juni	De uitzending van de kwalificatiewedstrijd voor het WK voetbal tussen Wales en Oekraïne wordt in Oekraïne onderbroken door een digitale aanval die gericht was op OLL.TV. Volgens SSSCIP hebben kwaadwillenden toegang verkregen tot een Content Delivery Network (CDN) en vervolgens het verkeer weten om te leiden. Als gevolg hiervan toonden verschillende Oekraïense tv-zenders Russische propaganda. [🔒]	4B
7 juni	De website van het Russische ministerie van Bouw, Huisvesting en Voorzieningen is beklad met het pro-Oekraïense bericht "Glory to Ukraine". De hackers vragen daarnaast een losgeldeis om te voorkomen dat ze mogelijk gestolen persoonsgegevens publiceren. [🔒]	4B, 4D, 6
14 juni	De Wit-Russische hacktivistische actor Belarusian Cyber Partisans claimt toegang te hebben tot getapte gesprekken van onder andere de Russische ambassade in Wit-Rusland. Het zou gaan om opnames tussen 2020 en 2021. [🔒]	2C, 4C

30 jun	Via een desinformatiecampagne wordt een gerucht verspreid dat Oekraïense mannelijke vluchtelingen in Polen zouden worden geïdentificeerd en teruggestuurd naar Oekraïne voor militaire dienst. De campagne wordt mogelijk uitgevoerd door de aan Wit-Rusland gelieerde actor GhostWriter. [🔓]	4A, 4C
19 juli	Google TAG merkt op dat Ghostwriter zich richt op social media-accounts van Poolse burgers, waarbij gebruik wordt gemaakt van de phishing-techniek "browser in the browser". [🔓]	4A
21 juli	Volgens de Oekraïense overheidsinstantie SSSCIP heeft een digitale aanval plaatsgevonden op de TAVR-mediagroep. Onder deze mediagroep vallen negen grote Oekraïense radiostations. De aanvallers hebben op de radio desinformatie verspreid over de gezondheid van de Oekraïense president Zelensky. [🔓]	4B
9 augustus	De website van het Finse parlement is getroffen door een DDoS-aanval. De pro-Russische hackersgroep NoName057(16) zegt achter de aanval te zitten. [🔓]	2C, 4D
11 augustus	Een DDoS-aanval vindt plaats op het Letse parlement. De digitale aanval gebeurde na het aannemen van een Letse verklaring die Rusland tot staatssponsor van terrorisme aanwijst. [🔓]	2C, 4D
13 augustus	Killnet zegt een DDoS-aanval te hebben uitgevoerd op defensieconcern Lockheed Martin. De groep zou ook persoonlijke gegevens hebben gestolen van medewerkers en dreigt deze gegevens te publiceren. [🔓]	2C, 4C
31 augustus	De overheid van Montenegro is slachtoffer geworden van een ransomware-aanval. Op zijn darkweb-leksite eist de Cuba ransomware-groep de verantwoordelijkheid voor de aanval op. [🔓]	4D, 6
7 september	KillNet claimt DDoS-aanvallen op Japanse organisaties. Hierdoor werden 20 overheidswebsites en het e-Gov, een webportaal voor burgers, geraakt. [🔓]	2C, 4D
5 oktober	Killnet claimt een aantal Amerikaanse overheidswebsites offline te hebben gehaald. Het betreft websites van de staten Colorado, Mississippi en Kentucky. De meeste getroffen websites waren op dezelfde dag weer online. [🔓]	2C, 4D
15 oktober	Pro-Russische hackers voeren DDoS-aanvallen uit op Bulgaarse (overheids)organisaties. Deze veroorzaakten kleine storingen, maar de schade bleef volgens de Bulgaarse overheid beperkt. Killnet zegt verantwoordelijk te zijn. [🔓]	2C, 4D
27 oktober	De parlementen van Polen en Slowakije zijn getroffen door digitale aanvallen. De Poolse Senaatsvoorzitter meldt dat de aanval mogelijk	4D

	verband houdt met een eerdere stemming die Rusland tot een "terroristisch regime" heeft verklaard. Volgens de plaatsvervangend voorzitter van het Slowaakse parlement vielen alle computers en telefoonlijnen van het parlement van Slowakije uit, waardoor het onmogelijk werd om over wetsvoorstellen te stemmen. [🔒]	
9 november	Een hack-en-lek operatie gericht op de overheid van Moldavië zorgt voor een politiek schandaal. Dit schandaal wordt door pro-Russische bewegingen aangegrepen om de zittende regering te ondermijnen. [🔒]	4C
14 november	Killnet claimt een DDoS-aanval op de website van de Amerikaanse FBI. [🔒]	2C, 4D
23 november	De website van het Europese Parlement is geraakt door een DDoS-aanval waar Killnet de verantwoordelijkheid voor claimt. De aanval vond plaats na een stemming in het parlement over het aanwijzen van Rusland als staatssponsor van terrorisme. [🔒]	2C, 4D

Dreigingscategorie 5: Statelijke economische spionage

Datum	Aanval	Dreigings-categorie
29 september	De Finse veiligheids- en inlichtingendienst SUPO waarschuwt voor mogelijk verhoogde Russische digitale spionageactiviteit aankomende winter. De waarschuwing hiervoor zou voortkomen uit een Russisch gebrek aan human intelligence (humint), omdat veel Russische diplomaten westerse landen zijn uitgezet. Ook vanwege de westerse sancties kan Rusland inlichtingen willen vergaren over de ontwikkeling van hoogwaardige technologie. [🔒]	3, 5

Dreigingscategorie 6: Digitale aanvallen voor financieel gewin

Datum	Aanval	Dreigings-categorie
april-mei	Verschillende publieke organisaties in Costa Rica zijn het slachtoffer geworden van digitale aanvallen waarbij gebruik wordt gemaakt van Conti-ransomware. Costa Rica verkeert in een nationale noodtoestand. [🔒] [🔒]	1, 6
3 mei	Google TAG meldt dat financieel-gemotiveerde actoren de oorlog als thema gebruiken voor bijvoorbeeld malafide mails en linkjes. [🔒]	2A, 6

17 juni	Killnet roept via Telegram verschillende ransomware-actoren als Conti en REvil op om gezamenlijk organisaties in de VS, Italië en Polen digitaal aan te vallen.	6
19 juli	Google TAG ziet een toename in het aantal financieel gemotiveerde actoren dat zich op Oekraïne richt. Een campagne van een groep die door CERT-UA wordt gevolgd als UAC-0098 leverde hiervoor documenten met de Follina-exploit, waarbij de groep zich voordeed als de Staatsbelastingdienst van Oekraïne. [🔒]	6
27 juli	CERT-UA waarschuwt voor phishing-mails, zogenaamd afkomstig van het Rode Kruis, waarin om donaties wordt gevraagd voor Oekraïense vluchtelingen. De berichten bevatten een linkje naar een phishing-site die een Oekraïense bank nabootst. Inloggegevens die op deze site worden ingevuld, belanden in de handen van de aanvallers. [🔒]	2B, 6
31 augustus	De overheid van Montenegro is slachtoffer geworden van een ransomware-aanval. Op hun darkweb-leksite eist de Cuba ransomware-groep de verantwoordelijkheid voor de aanval op. [🔒]	4D, 6
7 september	Google TAG neemt een toenemend aantal financieel gemotiveerde actoren waar die zich richten op Oekraïne en waarvan de activiteiten lijken op door de Russische overheid gesteunde hackers. Zo zijn sommige leden van de groep UAC-0098 voormalige Conti-leden die hun technieken nu inzetten op Oekraïense doelwitten. [🔒]	6
2 oktober	Volgens het Oekraïense nieuwsplatform *Kyiv Post* zouden Russische hackers van de National Republican Army (NRA) een ransomware-aanval op het Russische bedrijf Unisoftware hebben uitgevoerd. Volgens het platform zouden persoonlijke gegevens van klanten zijn gestolen. Ook de Russische overheid zou klant zijn van Unisoftware, volgens de *Kyiv Post*. De mobilisatie van Russische burgers zou aanleiding zijn geweest voor de aanval. [🔒]	6
24 oktober	CERT-UA publiceert een bericht over een phishing-campagne waarmee RomCom malware wordt geïnstalleerd. CERT-UA acht het mogelijk dat de campagne verband houdt met UNC2596/Tropical Scorpius – de actor achter Cuba-ransomware. [🔒]	6
28 november	ESET maakt melding van de inzet van RansomBoggs-ransomware, mogelijk door de Russische statelijke actor Sandworm, tegen Oekraïense organisaties. [🔒]	6

Uitgave
Nationaal Cyber Security Centrum (NCSC)
Postbus 117, 2501 CC Den Haag
Turfmarkt 147, 2511 DP Den Haag
070 751 5555

Meer informatie
www.ncsc.nl
info@ncsc.nl
@ncsc_nl

december 2022

TLP: AMBER