EUROPE

Daderprofielen van cybercriminelen uit Oost-Europa en Rusland

Fook Nederveen, Erik Silfversten, Rick Slootweg, Stijn Hoorens

For more information on this publication, visit www.rand.org/t/RRA3346-1

About RAND Europe
RAND Europe is a not-for-profit research organisation that helps improve policy and decision making through research and analysis. To learn more about RAND Europe, visit www.randeurope.org.

Research Integrity
Our mission to help improve policy and decision making through research and analysis is enabled through our core values of quality and objectivity and our unwavering commitment to the highest level of integrity and ethical behaviour. To help ensure our research and analysis are rigorous, objective, and nonpartisan, we subject our research publications to a robust and exacting quality-assurance process; avoid both the appearance and reality of financial and other conflicts of interest through staff training, project screening, and a policy of mandatory disclosure; and pursue transparency in our research engagements through our commitment to the open publication of our research findings and recommendations, disclosure of the source of funding of published research, and policies to ensure intellectual independence. For more information, visit www.rand.org/about/principles.

RAND's publications do not necessarily reflect the opinions of its research clients and sponsors.

Published by the RAND Corporation, Santa Monica, Calif., and Cambridge, UK

© 2024 RAND Corporation

RAND® is a registered trademark.

Limited Print and Electronic Distribution Rights
This publication and trademark(s) contained herein are protected by law. This representation of RAND intellectual property is provided for noncommercial use only. Unauthorised posting of this publication online is prohibited; linking directly to its webpage on rand.org is encouraged. Permission is required from RAND to reproduce, or reuse in another form, any of its research products for commercial purposes. For information on reprint and reuse permissions, please visit www.rand.org/pubs/permissions.

Cover: Adobe Stock

© 2024 RAND Europe. Auteursrechten voorbehouden. Niets uit dit rapport mag worden verveelvoudigd en/of openbaar gemaakt door middel van druk, fotokopie, microfilm, digitale verwerking of anderszins, zonder voorafgaande schriftelijke toestemming van RAND Europe.

Voorwoord

Cybercrime kan organisaties van alle groottes en in alle sectoren treffen. Veel grootschalige, high-impact cybercrime-incidenten van de afgelopen jaren komen vanuit Oost-Europa. Het gaat daarbij voornamelijk om ransomware. De daders lijken vooral uit Rusland en Oekraïne, maar ook uit Roemenië, Georgië, Moldavië en Bulgarije, afkomstig te zijn. De oorlog tussen Rusland en Oekraïne heeft deze dreiging complexer gemaakt, doordat cybercriminelen in de regio gemakkelijker buiten het zicht van de autoriteiten opereren. Hoewel veel informatie is verzameld over de operaties, modi operandi, impact en slachtoffers van cybercrime, is veel minder bekend over de daders.

Om bestaande kennis over de daderprofielen van deze groep cybercriminelen in kaart te brengen, heeft het Wetenschappelijk Onderzoeks- en Datacentrum (WODC) een kennistafel laten organiseren. Aan een kennistafel worden deskundigen bijeengebracht om de bestaande kennis en de kennisbehoefte rondom een bepaald onderwerp op basis van een groepsgesprek in kaart te brengen. De resultaten kunnen richting geven aan toekomstig onderzoek en beleidskeuzes. Aan deze kennistafel is gekeken naar de achtergrondkenmerken, drijfveren en rekrutering van deze groep cybercriminelen en naar hiaten in deze kennis. Een verbeterde kennispositie kan bijdragen aan de inspanningen van het Ministerie van Justitie en Veiligheid, het Openbaar Ministerie en de politie om cybercrime te bestrijden en voorkomen.

De kennistafel is georganiseerd door RAND Europe, een onafhankelijk not-for-profit onderzoeksbureau voor beleidsonderzoek met als missie beleid en besluitvorming te verbeteren. Dit rapport presenteert de bevindingen van de kennistafel. We willen de experts die hun kennis aan de kennistafel hebben gedeeld hartelijk bedanken. Ook bedanken we dr. Saskia Baas van het WODC voor de projectbegeleiding, dr. Henk van der Veen (WODC) en Laetitia Kröner (Ministerie van Justitie en Veiligheid) voor hun constructieve feedback op het verslag, en Joe Uchill voor zijn onderzoeksassistentie.

Dit rapport heeft, conform de kwaliteitsstandaarden van RAND, peer review ondergaan voor kwalitatief hoogstaand onderzoek. We bedanken onze collega's Erik Frinking en dr. Henri van Soest voor hun opbouwend commentaar. De auteurs dragen de verantwoordelijkheid voor de inhoud van dit rapport. Voor meer informatie over dit rapport of RAND Europe kunt u contact opnemen met Fook Nederveen (fook_nederveen@randeurope.org).

RAND Europe
Rotterdam Building
Aert van Nesstraat 45
3012 CA, Rotterdam
Nederland
Tel. +31 10 899 5916

RAND Europe
Rue de la Loi 82
Bus 3
1040 Brussel
België
Tel. +32 2669 2400

RAND Europe
Eastbrook House
Shaftesbury Road
Cambridge CB2 8DR
United Kingdom
Tel. +44 1223 353 329

Samenvatting

Veel grootschalige, high-impact cybercrime-incidenten van de afgelopen jaren komen vanuit Oost-Europa, met name uit Rusland en Oekraïne, maar ook uit Roemenië, Georgië, Moldavië en Bulgarije. Voorbeelden van cybercrime-incidenten zijn hacken, DDoS-aanvallen en ransomware. Momenteel speelt met name ransomware in deze context een rol. De cyberdreiging uit deze regio kan toenemen als de oorlog tussen Rusland en Oekraïne verder escaleert.

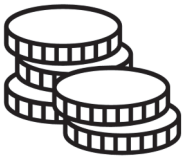
Hoewel veel onderzoek is gedaan naar de activiteiten van georganiseerde cybercriminaliteit en de tactieken, technieken en procedures die worden gebruikt om illegale activiteiten uit te voeren, is veel minder bekend over de daderprofielen van de cybercriminelen die hierbij betrokken zijn. In deze context heeft het Wetenschappelijk Onderzoek- en Datacentrum aan RAND Europe gevraagd een kennistafel te organiseren om bestaande kennis over de achtergrondkenmerken, drijfveren en rekrutering van deze groep cybercriminelen, en de hiaten in deze kennis, in kaart te brengen. Een verbeterde kennispositie kan bijdragen aan de inspanningen van het Ministerie van Justitie en Veiligheid, het Openbaar Ministerie en de politie om cybercrime te bestrijden en te voorkomen.

Afbakening en opzet van de kennistafel

De reikwijdte van de kennistafel was beperkt tot georganiseerde, high-impact, cyberafhankelijke criminaliteit afkomstig uit Oost-Europa. Gedigitaliseerde criminaliteit, zoals online fraude en de handel in illegale goederen via het dark web, en door een staat gesteunde cyberspionage vallen buiten de aandacht van de kennistafel.

Acht deskundigen uit de academische wereld, rechtshandhaving en cybersecurity met expertise in het opsporen en onderzoeken van deze groep cybercriminelen namen deel aan de kennistafel. Samen brachten zij de beschikbare kennis over achtergrondkenmerken, drijfveren en rekrutering in kaart. Deze drie aandachtsgebieden waren onderverdeeld in verschillende aspecten, te zien in Figuur 1. Voor elk aspect beoordeelden de deskundigen, na een discussie over de kennis en de hiaten daarin, het kennisniveau op dat aspect aan de hand van enkele scoringscriteria. De deskundigen konden kiezen uit 'hoog', 'matig', 'beperkt' of 'onbekend'. De resultaten werden daarna getoond op een scherm en collectief besproken. In dit eindverslag van de kennistafel zijn de gedeelde inzichten geaggregeerd op groepsniveau.

Figuur 1. Aandachtsgebieden en aspecten



Achtergrondkenmerken van deze groep cybercriminelen	Drijfveren van deze groep cybercriminelen	Rekrutering door cybercriminele groepen
• Demografische kenmerken • Sociaaleconomische kenmerken • Vrijetijdsbesteding • Gezins- en thuissituatie • Psychologische kenmerken en zelfbeeld • Sociale contacten • Criminele verleden en carrière	• Economische drijfveren • Sociale drijfveren • Intellectuele drijfveren • Psychologische en gedragsmatige drijfveren • Politieke drijfveren	• Rekruteringstrategieën • Arbeidsvoorwaarden en werkomstandigheden • Vereiste vaardigheden en ervaring

Bevindingen

Om inzichten te verzamelen over deze groep cybercriminelen zijn verschillende databronnen en onderzoeksmethoden beschikbaar. Voorbeelden hiervan zijn opsporingsgegevens, interviews met daders of opsporings- en inlichtingenambtenaren, enquêtes onder slachtoffers, analyses van cybercriminele marktplaatsen, fora en gelekte chats, casestudies, psycholinguïstische analyses van digitale communicatie, misdaadscripts, gedragsanalyses en typologieën van hackers. Dit eindverslag biedt inzicht in de ervaringen van enkele vooraanstaande deskundigen in het onderzoeken van deze groep cybercriminelen.

Wat betreft achtergrondkenmerken van de waarschijnlijk tienduizenden betrokkenen gaven de deskundigen aan dat de meesten man zijn. Leeftijd en nationaliteit zouden vaak in verband gebracht kunnen worden met het soort cybercriminele activiteiten dat zij bezigen. Wanneer ze beginnen met cybercrime lijken ze geen strafblad te hebben, noch lijken ze zich in parallel met andersoortige misdaad bezig te houden. Over het algemeen zouden ze vaak hoog opgeleid zijn. In hun vrije tijd lijken ze vaak computergerelateerde hobby's te hebben. Vertrouwensproblemen en autisme zouden veel voorkomen bij deze groep. Ten slotte werd geconstateerd dat alhoewel de criminelen georganiseerd te werk gaan, de samenwerkende personen elkaar maar zelden fysiek lijken te ontmoeten.

Volgens de deskundigen is financieel gewin de voornaamste drijfveer voor deze groep cybercriminelen. Vrijwel alle diensten en vaardigheden worden tegen betaling aangeboden. In vergelijking met het Westen is de werkgelegenheid in Oost-Europa lager, betalen IT-banen minder en is er weinig sociale zekerheid. Cybercrime kan aantrekkelijk zijn vanwege het lage risico om gepakt te worden en de grote financiële beloningen die het biedt. Niettemin spelen andere drijfveren ook een rol. Individuen worden waarschijnlijk gemotiveerd door een combinatie van factoren.

Tot slot stelden de deskundigen vast dat rekrutering voornamelijk op online fora plaatsvindt. In sommige gevallen zijn formele wervingsprocedures opgetuigd, waar kandidaten hun cv, motivatiebrief, referenties en een overzicht van Bitcoin-portefeuilles moeten aanleveren. Het komt ook voor dat kandidaten bepaalde tests moeten volbrengen om hun vaardigheden te bewijzen. Reputatie lijkt een belangrijk element in het wervingsproces. Potentiële medewerkers moeten aantonen dat zij eerder betrokken zijn geweest bij cybercriminele activiteiten, waarbij gemeenschappelijke contacten een belangrijke rol spelen. Meestal wordt op freelancebasis gewerkt.

Uit de beoordelingen door de deskundigen blijkt dat het kennisniveau rondom drijfveren en rekrutering van de groep cybercriminelen over het algemeen hoger is dan rondom achtergrondkenmerken. De kennis is uitgebreider en sterker wanneer het minder noodzakelijk is om informatie te linken aan de identiteit van specifieke personen (zogenaamde 'pre-attributiegegevens'). Zo is het lastig data te verzamelen over de gezinssituaties van de daders, als niet is vastgesteld om welke personen het gaat. Voor aspecten waar dat minder noodzakelijk is, is het ook eenvoudiger om inzichten te verwerven. Over de vrijetijdsbesteding van cyberdaders is bijvoorbeeld veel informatie te vinden, omdat ze hier online opener over spreken en sporen van achterlaten.

De vele inzichten die de deskundigen aan de kennistafel deelden over de daderprofielen van cybercriminelen uit Oost-Europa staan in schril contrast met de beperkt beschikbare academische literatuur. Uit de kennistafel is gebleken dat de dekking en bewijskracht van de beschikbare kennis over de verschillende elementen uit de daderprofielen van cybercriminelen die actief zijn vanuit Oost-Europa uiteenlopen. Hoewel over alle aspecten van cybercrime enige informatie bekend is, is de beschikbare kennis tegelijkertijd verre van compleet. Dit kan leiden tot een vertekend beeld. Bovendien is de basis van de verzamelde inzichten niet gevalideerd in dit onderzoek. Het kan niet worden uitgesloten dat de informatie waarop dit rapport gebaseerd is niet representatief is.

Toekomstig onderzoek

Aan de hand van toekomstig onderzoek kunnen de daderprofielen nader in kaart worden gebracht. Bij georganiseerde cybercriminaliteit zijn veel verschillende typen personen betrokken. Kennisvereisten en hiaten in kennis over deze groep cybercriminelen lopen dan ook uiteen. Deze zijn bijvoorbeeld afhankelijk van de rollen die ze vervullen in de organisatie, of van het doel van de benodigde informatie, zoals opsporing, vervolging of preventie.

De aspecten met het laagste kennisniveau verdienen niet automatisch prioriteit voor toekomstig onderzoek. Evenmin is op dit moment voldoende informatie beschikbaar voor de aspecten waarvoor het kennisniveau als hoger wordt beschouwd. Belangrijke factoren zijn onder andere de haalbaarheid van het achterhalen van informatie en of de inzichten nuttig zijn zonder samenwerking met de lokale autoriteiten.

Om cybercriminelen effectiever te bestrijden, zijn aanvullende data en inzichten het nuttigst over de volgende aspecten, in willekeurige volgorde:

- Het criminele verleden van de cybercriminelen;
- De sociale en psychologische drijfveren die een rol spelen bij technisch onderlegde personen die cybercrimineel worden in plaats van een legaal beroep in het IT-veld kiezen;

- De fora en andere platforms waarop de cybercriminelen actief zijn en de belangrijkste communicatiekanalen die cybercriminelen op een bepaald moment gebruiken;
- Hoe cybercriminelen samenwerken en hun onderlinge rivaliteit;
- De relaties tussen de cybercriminelen en de politiek en ideologische motivaties;
- In hoeverre cybercriminelen samenwerken met inlichtingendiensten en overheidsorganisaties in Rusland en Oekraïne; en
- De manieren waarop geld wordt witgewassen.

Op deze gebieden is met name meer onderzoek op basis van primaire data, zoals politiedata, gelekte chatlogs, via fora, etnografisch onderzoek en kwalitatieve interviews, van toegevoegde waarde. Ook kan toekomstig onderzoek dieper ingaan op hoe verschillende persoonlijkheidskenmerken gekoppeld kunnen worden aan verschillende rollen binnen de groepen en gemeenschap. Daarnaast kan nader onderzoek helpen verduidelijken 1) welke kennis het meest nuttig is voor verschillende doeleinden, zoals preventie of opsporing; 2) hoe cyberdaders in het verlengde daarvan het best geprofileerd kunnen worden; en 3) hoe opgedane kennis over daderprofielen van cybercriminelen geïntegreerd kan worden in het technisch en digitaal forensisch onderzoek.

Inhoud

Voorwoord i
Samenvatting ii
Inhoud vi
1. Inleiding 1
1.1. Achtergrond 1
1.2. Onderzoeksvragen 2
1.3. Afbakening 3
1.4. Methodologie 4
1.5. Leeswijzer 5
2. Achtergrondkenmerken 7
3. Drijfveren 14
4. Rekrutering 18
5. Kennishiaten en toekomstig onderzoek 21
Bronnen 24

Tabellen

Tabel 1. Scoringscriteria voor de kennisbeoordeling 5

Figuren

Figuur 1. Aandachtsgebieden en aspecten iii
Figuur 2. Overzicht van de kennisbeoordeling door de deskundigen 22

Kaders

Kader 1. Bevindingen van de kennistafel over achtergrondkenmerken 8
Kader 2. Bevindingen van de kennistafel over drijfveren 14
Kader 3. Bevindingen van de kennistafel over rekrutering 19

1. Inleiding

In dit hoofdstuk presenteren we de achtergrond waartegen de kennistafel is uitgevoerd (Paragraaf 1.1), de onderzoeksvragen (Paragraaf 1.2), de afbakening (Paragraaf 1.3) en de gehanteerde methodologie (Paragraaf 1.4).

1.1. Achtergrond

Opsporingsdiensten in Nederland krijgen vaak en veel te maken met cyberdreigingen (Politie 2023). Deze dreiging wordt vergroot door de steeds verdere professionalisering van zware, georganiseerde cybercrime. Bij cybercrime-incidenten kan men denken aan ransomware,[1] hacken[2] en Distributed-Denial-of-Service (DDoS)-aanvallen.[3] Onder andere de Nationaal Coördinator Terrorismebestrijding en Veiligheid (NCTV) stelt dat Oost-Europa, en specifiek Rusland en Oekraïne, opvalt als een belangrijke hub van ernstige cybercrime-activiteiten die zich richten op Nederland en andere landen (CISA 2022; IISS 2023; Joint Cybersecurity Advisory 2022; NCTV 2023). De oorlog in Oekraïne maakt het voor (cyber)criminelen in de regio gemakkelijker om buiten het zicht van de autoriteiten te opereren. Bovendien betekende de verslechtering van de betrekkingen tussen NAVO-landen en Rusland sinds de jaren 2010 ook een breuk in de samenwerking tussen Europese en Amerikaanse rechtshandhavingsinstanties enerzijds, en het Russische ministerie van Binnenlandse Zaken anderzijds. Hierdoor konden Russische cybercriminele groeperingen praktisch ongestraft optreden, of zelfs met steun van de overheid, volgens onder andere de Amerikaanse overheidsdienst Cybersecurity and Infrastructure Security Agency (CISA 2022; Glenny 2023).[4]

Volgens CISA hebben meerdere cybercriminele groepen die voorheen min of meer onafhankelijk opereerden, zoals de groep bekend als 'Wizard Spider', sinds het begin van de Russische invasie in Oekraïne in februari 2022 hun steun uitgesproken voor de Russische staat (CISA 2022; Felbab-Brown & Paz García 2024). Andere groepen zouden hun steun hebben uitgesproken aan Oekraïne. Omdat hackersgroepen

[1] Ransomware is schadelijke software die een apparaat en/of de gegevens die erop staan permanent vergrendelt, tenzij het slachtoffer losgeld betaalt.

[2] Hacken is een breed begrip. In de context van cybercrime gaat het om het inbreken in computersystemen, netwerken, digitale apparaten of persoonlijke accounts om deze uit te buiten.

[3] Bij een DDoS-aanval worden online diensten of de ondersteunende servers en netwerkapparatuur overbelast en verstoord door een overvloed aan internetverkeer.

[4] Men denkt dat de Russische staat cybercrime gericht op buitenlandse doelwitten toestaat, mits criminelen geen binnenlandse doelwitten aanvallen. Een veelgebruikte tactiek is het ontwerpen van malware die niet wordt geïnstalleerd op systemen met Cyrillische toetsenborden (Chainanalysis 2021).

online opereren, bestaan deze niet altijd uit individuen met dezelfde nationaliteit. De herpositionering leidde daarom tot onenigheid binnen sommige van deze groepen en tot het overlopen van enkele individuen van de ene naar de andere groep (Mandiant 2023; Recorded Future 2023).

De NCTV merkt in het Cybersecuritybeeld Nederland 2023 (CSBN 2023) op dat de Russische cybersabotage van Oekraïne de grootste in de geschiedenis is. Tot nu toe richtten Russische cyberaanvallen, zoals spionage, sabotage en desinformatie, zich voornamelijk op Oekraïne en de regio. Volgens het CSBN 2023 zijn er geen cyberaanvallen geweest die de Nederlandse samenleving of nationale veiligheid ernstig hebben ontwricht. Cybercrime-incidenten in Nederland waren divers van aard, al bleef ransomware een prominente rol spelen (NCTV 2023). In bepaalde gevallen werd de gestolen informatie gepubliceerd, wat resulteerde in zowel materiële schade als reputatieschade. Een voorbeeld hiervan is de ransomware-aanval op verschillende Nederlandse woningcorporaties uit 2022, waarbij de cybercriminele groep Conti onder andere kopieën van paspoorten en rijbewijzen publiceerde (Verlaan 2022).

Volgens de NCTV (2023) kan het feit dat zich geen maatschappij-ontwrichtende cyberaanvallen hebben voorgedaan in Nederland snel veranderen als de oorlog tussen Rusland en Oekraïne verder escaleert. De NCTV adviseert daarom waakzaam te zijn voor cascade-effecten die invloed hebben op vitale processen en voor aanvallen door bijvoorbeeld pro-Russische criminelen. De vervaging van bedreigingen die primair 'crimineel' of 'statelijk' van aard zijn, werd ook opgemerkt door het Amerikaanse Ministerie van Justitie, dat stelde: '*criminal actors and nation states are forming alliances of convenience, alliances of opportunity, and sometimes alliances by design*' (US Department of Justice 2021, 11). Het ministerie noemt de toename van ransomware-aanvallen uit winstbejag op vitale infrastructuurnetwerken, zoals ziekenhuizen, door transnationaal georganiseerde cybercriminele groepen uit Rusland en Oost-Europa als voorbeeld van hoe de cyberdreiging zich vermengt. Een voorbeeld hiervan in Nederland zijn de DDoS-aanvallen in 2023, opgeëist door de Russische criminele groep NoName057(16), op verschillende Nederlandse organisaties, waaronder Maastricht Aachen Airport, OV-NL, bedrijven in de havens van Delfzijl en Eemshaven, gemeenten en de Nederlandse Kamer van Koophandel, als vergelding voor de Nederlandse steun aan Oekraïne (Privacy-web 2023).

Cybercrime kan organisaties van alle groottes en in alle sectoren treffen (CBS 2023). De Nederlandse Algemene Inlichtingen- en Veiligheidsdienst (AIVD) stelde in zijn Jaarverslag 2022 dat de bijbehorende risico's 'enorm' zijn voor de overheid, bedrijven, kennisinstellingen en het grote publiek (AIVD 2023). De inval in Oekraïne heeft een impuls gegeven aan de Nederlandse inspanningen om de maatschappelijke cyberweerbaarheid te verbeteren (IISS 2023). Om georganiseerde cybercrime te bestrijden, is het van cruciaal belang te begrijpen wie de cybercriminelen zijn. RAND Europe concludeerde in 2019 dat dit een prioriteit moet zijn voor de onderzoeksagenda op het gebied van cybersecurity (Silfversten et al. 2019). Hoewel veel informatie is verzameld over de operaties, modus operandi, impact en slachtoffers van cybercrime, is veel minder bekend over de daders van deze criminele activiteiten (Bada & Nurse 2021; Martineau et al. 2023).

1.2. Onderzoeksvragen

Op verzoek van het Ministerie van Justitie en Veiligheid en het Openbaar Ministerie heeft het Wetenschappelijk Onderzoeks- en Datacentrum (WODC) RAND Europe gevraagd een kennistafel te

organiseren om bestaande kennis rondom de daderprofielen van cybercriminelen die opereren vanuit Oost-Europa in kaart te brengen. **Het doel van de kennistafel was tot een overzicht van de beschikbare kennis en de hiaten daarin te komen**. De volgende onderzoeksvragen waren leidend voor de kennistafel:

1) Wat is bekend over de **achtergrondkenmerken** (leeftijd, opleidingsniveau, etc.) van deze groep cybercriminelen?
2) Wat is bekend over de **drijfveren** van deze groep cybercriminelen?
3) Op welke wijze worden deze cybercriminelen **gerekruteerd** door cybercriminele groeperingen?
4) Welke **kennishiaten** zijn er rondom deze groep cybercriminelen en welk onderzoek is nodig om deze op te vullen?

Een verbeterde kennispositie draagt bij aan de inspanningen om de Nederlandse overheid, met name het Ministerie van Justitie en Veiligheid, de politie en het Openbaar Ministerie, beter in staat te stellen cybercrime te bestrijden en voorkomen.

1.3. Afbakening

De kennistafel is uitsluitend gericht op cyberafhankelijke criminaliteit (of *cyber-dependent crime*)**.** Dit zijn misdrijven waarbij IT-systemen zowel als aanvalsmiddel als doelwit worden gebruikt, zoals malware, ransomware, hacken en DDoS-aanvallen. Soms wordt ook gedigitaliseerde criminaliteit (of *cyber-enabled crime*) onder cybercrime geschaard. Daarbij gaat het om traditionele, offline misdrijven die qua omvang of vorm zijn getransformeerd via het internet, zoals online fraude, online intimidatie en handel in illegale goederen via het dark web. Deze vormen van cybercrime vallen buiten de aandacht van de kennistafel. De nadruk ligt daarnaast op activiteiten die hoofdzakelijk crimineel zijn. Dit is een onscherpe afbakening vanwege de bovengenoemde vervaging van 'criminele' en 'statelijke' dreigingen. Door een staat gesteunde cyberspionage of tactieken, technieken en procedures vallen bijvoorbeeld buiten de reikwijdte van de kennistafel.

De kennistafel is uitsluitend gericht op cyberdaders afkomstig uit Oost-Europa. De verantwoordelijken voor de grootste incidenten van cybercrime in Nederland blijken vaak afkomstig uit deze regio. Zo zijn veel in de afgelopen jaren gearresteerde hackers van Russische, Oekraïense, Roemeense, Georgische, Moldavische en Bulgaarse afkomst (Peer 2023). Cyberdreigingen uit andere landen en regio's die eveneens prominent zijn en de aandacht verdienen, zoals uit China, worden voor deze kennistafel buiten beschouwing gelaten omdat de aard van de dreiging en de daders uiteenloopt. Door de kennistafel te richten op Oost-Europa is de kennis gerichter en nauwkeuriger voor die specifieke groep daders.

De kennistafel is gericht op georganiseerde, high-impact cybercrime. Voorbeelden van relevante, beruchte criminele groepen uit de regio zijn, in alfabetische volgorde: Cl0p, Conti, Cosmic Lynx, The CoomingProject, DarkSide, Evil Corp, FIN7, Lockbit, Mummy Spider, Revil, Salty Spider, Scully Spider, Smokey Spider, Wizard Spider en Xaknet (CISA 2022). Deze groepen hanteren verschillende tactieken en zijn opportunistisch in het selecteren van hun doelwitten. Momenteel zetten zij vooral ransomware in: het uitschakelen van systemen, meestal door bestanden te versleutelen, totdat losgeld wordt betaald. Sommige groepen voegen daar een tweede afpersingstechniek aan toe, door te dreigen met het lekken van bestanden.

Andere groepen, zoals Karakurt, Donut en BianLian, zijn overgestapt op afpersing zonder encryptie en gebruiken alleen de dreiging van lekken (Zscaler 2023).

1.4. Methodologie

Het hoofdonderdeel van dit onderzoek betrof de organisatie van een kennistafel om de bovengenoemde onderzoeksvragen te beantwoorden. **Acht deskundigen** met ruime academische en/of praktijkervaring op het gebied van Oost-Europese cybercrime hebben deelgenomen aan de hybride kennistafel op 9 april 2024 in Den Haag. Wij zijn deze deskundigen erkentelijk voor de nuttige en inzichtelijke bijdragen. Wij bedanken, op alfabetische volgorde van achternaam, Jildau Borwell (Team Cybercrime Noord-Nederland, Politie & Haagse Hogeschool), Jon DiMaggio (Analyst1), John Fokker (Threat Intelligence, Trellix), Michael Levi (Cardiff University), Martijn Peijer (Security Operations Center, Belastingdienst), een anonieme deelnemer van de Shadowserver Foundation, en twee deelnemers die geheel anoniem wensen te blijven.

Voorafgaand aan de kennistafel stelden wij een **korte memo** op, met een samenvatting van de (beperkt) beschikbare literatuur en een uitleg van de opzet en onderzoeksvragen van de kennistafel. Een week voorafgaand aan de kennistafel werd deze memo gedeeld met de deelnemers. De memo en de kennistafel waren gestructureerd aan de hand van de drie aandachtsgebieden binnen de onderzoeksvragen: achtergrondkenmerken, drijfveren en rekrutering. Om de kennistafel te structureren en een goede dekking van de informatie te verzekeren, is elk aandachtsgebied opgesplitst in enkele aspecten.

Voor elk van de drie aandachtsgebieden werden vier gefaciliteerde stappen doorlopen:

1) In stap 1 presenteerden wij onze onderverdeling in aspecten, en voerden de deskundigen een discussie over de compleetheid en geschiktheid daarvan en de noodzaak van eventuele herzieningen.
2) In stap 2 stelden wij de groep per aspect de open vraag wat daarover, op basis van de bestaande kennis, gezegd kan worden voor cybercriminelen die opereren vanuit Oost-Europa.
3) In stap 3 scoorden de deskundigen individueel hun inschatting van het niveau van de huidige kennis met behulp van een interactieve tool. De resultaten werden direct verwerkt en op een scherm gedeeld.
4) In stap 4 bespraken we gezamenlijk de resultaten van het scoren. De deskundigen lichtten hun keuze toe en de andere aanwezigen konden hierop reageren, bijvoorbeeld met aanvullingen of nuanceringen. Ook verwelkomden we aanvullende opmerkingen of inzichten over hiaten in de kennis.

Voor het scoren van de bewijskracht hebben wij enkele **scoringscriteria** opgesteld. Tabel 1 toont de vier opties waaruit de deelnemers konden kiezen bij hun inschatting van het kennisniveau: hoog, matig, beperkt of onbekend.

Tabel 1. Scoringscriteria voor de kennisbeoordeling

		Kenniskenmerken			
		Volledigheid	**Beschikbaarheid van bronnen**	**Soorten bronnen**	**Consistentie**
Bewijskracht	**Hoog**	Volledige dekking van belangrijke aspecten, bekende feiten	Uitgebreide en gevarieerde bronnen	Uitgebreid bewijsmateriaal; uitgebreide opsporingsdata; academisch (peer-reviewed) onderzoek	Zeer consistent
	Matig	Belangrijkste aspecten worden behandeld, bekende onbekenden	Adequate bronnen op sommige gebieden	Incidenteel bewijsmateriaal; informatie van inlichtingendiensten	Grotendeels consistent
	Beperkt	Enige dekking van belangrijke aspecten, onbekende onbekenden	Beperkte bronnen	Anekdotische informatie; enige informatie van inlichtingendiensten; journalistieke verslaggeving	Enigszins consistent, enigszins tegenstrijdig bewijs
	Onbekend	Meeste belangrijke aspecten niet gedekt, onkenbare onbekenden	Zeer beperkte of geen bronnen	Pure speculatie	Weinig consistentie, geen ondersteuning voor bevindingen

Bron: Geïnspireerd door het raamwerk van Pearce (2018).

1.5. Leeswijzer

In deze verslaglegging van de kennistafel leiden we elk aandachtsgebied kort in, waarna we **de bevindingen van de kennistafel presenteren in grijze kaders**. De bevindingen worden niet toegeschreven aan individuele deelnemers, maar geaggregeerd op groepsniveau. De bevindingen worden gepresenteerd per onderliggend aspect. Iedere paragraaf begint met een staafdiagram die de scores weergeeft. De totalen zijn niet altijd gelijk aan acht, omdat sommige deelnemers later aansloten of de kennistafel eerder moesten verlaten. Bovendien was antwoorden niet verplicht.

De bevindingen in de grijze kaders geven de inzichten, inschattingen en verwachtingen weer van de deskundigen op basis van hun onderzoekservaringen. Tijdens de kennistafel lag de nadruk op de kennis die de deelnemers vergaard hebben over de daders, niet op de beperkingen van de onderliggende data. De deskundigen hebben bijvoorbeeld veel inzichten opgedaan over de personen achter cybercriminele activiteiten op basis van onderlinge interactie in gelekte chats. Deze inzichten zijn opgenomen in de kaders, maar lastig te valideren omdat de betrouwbaarheid van de interactie op dergelijke chatfora niet kan worden vastgesteld. Het is mogelijk dat cybercriminelen liegen, opscheppen of bepaalde zaken verhullen. De meest uitgesproken personen zijn oververtegenwoordigd in de data, terwijl men van personen hogerop in een criminele organisatie een meer terughoudende houding zou kunnen verwachten. Zo zitten potentiële vertekeningen in deze data en beperkingen aan de inzichten die kunnen worden ontleend aan gesprekken op fora of interviews met cyberdaders.

De volgende hoofdstukken gaan achtereenvolgens in op de bevindingen van de kennistafel over de achtergrondkenmerken (**Hoofdstuk 2**), drijfveren (**Hoofdstuk 3**) en rekrutering (**Hoofdstuk 4**) van cybercriminelen die opereren vanuit Oost-Europa. Tot slot bespreken we in **Hoofdstuk 5** de voornaamste kennishiaten en welk onderzoek nodig is om deze op te vullen.

2. Achtergrondkenmerken

Tot nu toe is beperkt onderzoek gedaan naar persoonlijkheidsaspecten van cybercriminelen, ongeacht het land van herkomst of de regio van waaruit zij opereren. Martineau et al. (2023) concluderen in hun systematische review van literatuur over cyberprofilering dat dit veld nog in de kinderschoenen staat. Enkele jaren geleden deden Van der Wagen et al. (2019) in opdracht van het WODC onderzoek naar de daderprofielen van cybercriminelen in het algemeen, en hoe deze kenmerken zich verhouden tot die van daders van 'traditionele' criminaliteit. Zij maakten binnen de categorie achtergrondkenmerken de volgende onderverdeling:

1) Demografische kenmerken (o.a. leeftijd, sekse, etniciteit en woonplaats);
2) Sociaaleconomische kenmerken (o.a. sociaaleconomische status, sociale omgeving, opleidingsniveau en werkgelegenheid);
3) Vrijetijdsbesteding (o.a. hobby's, gewoonten, routines en lifestyle);
4) Gezins- en thuissituatie (o.a. gezinssituatie, relatie met ouders en ouderlijk toezicht en gezinsproblemen);
5) Psychologische kenmerken en zelfbeeld (o.a. intelligentie, verslavingen en persoonlijkheidsstoornissen);
6) Sociale contacten (o.a. vriendschappen, het hebben van delinquente vrienden en rolmodellen en sociale isolatie).

Deze categorieën hebben wij ook in de kennistafel aangehouden, aangevuld met de categorie:

7) Criminele verleden en carrière.

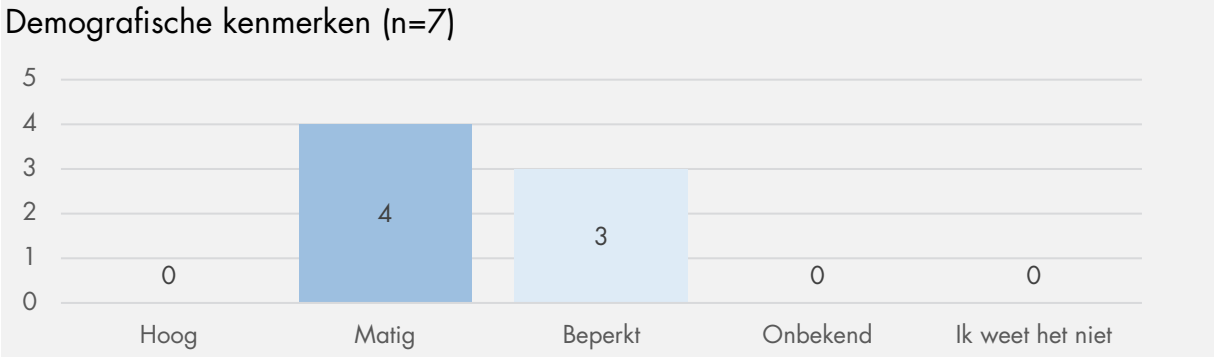
Deze categorie omvat het type criminele antecedenten en de ernst daarvan, de frequentie, het strafrechtelijk begin en hun criminele netwerk. Van der Wagen et al. (2019) beschouwen dit als losstaand onderwerp en wijden hier een apart hoofdstuk aan. Informatie over het criminele verleden en de carrière van de daders kan niettemin nuttig zijn voor risicoanalyses en het ontwikkelen van passende interventies om recidive te voorkomen (Huisman 2019). Daarom is het hier opgenomen onder achtergrondkenmerken.

Informatie verkrijgen over bepaalde achtergrondkenmerken van de daders is ingewikkeld door de complexe versleuteling waar cybercriminelen achter schuilgaan om anoniem te blijven, en het beperkte aantal veroordelingen. Om deze kenmerken toch te bestuderen, gebruiken onderzoekers en professionals op het gebied van cybercrime verschillende methodologische benaderingen. Voorbeelden zijn interviews met daders of opsporings- en inlichtingenambtenaren, enquêtes onder slachtoffers, analyses van cybercriminele

marktplaatsen, fora en gelekte chats, casestudies, psycholinguïstische analyses van digitale communicatie, misdaadscripts, gedragsanalyses, typologieën van hackers en, in zeldzame gevallen, het gebruik van gegevens uit onderzoeken van rechtshandhavingsinstanties (Bada & Nurse 2021; Lusthaus et al. 2023; Martineau et al. 2023). Mede door het gebrek aan grote beschikbare datasets of toegang tot een grote representatieve steekproef van daders, leunen de meeste academische studies op casestudies van daders achter specifieke aanvallen of bedreigingen (Bada & Nurse 2021). Het gebrek aan gegevens kan echter leiden tot onjuiste aannames over de achtergrondkenmerken van daders.

Binnen de overkoepelende groep cybercriminelen die opereert vanuit Oost-Europa lopen de achtergrondkenmerken van verschillende subgroepen uiteen. Zo zijn verschillen in gedrag en de sociale contacten van kernleden van een groep, de personen die deel uitmaken van grote netwerken, en opkomende cybercriminelen. Dat kan eveneens bepalend zijn voor waar kennishiaten exact zitten. Om tot een algemeen overzicht te komen, werd de deelnemers gevraagd zoveel mogelijk met helikopterblik naar de groep als geheel te kijken, en de opmerkelijkste verschillen en hiaten voor bepaalde groepen of categorieën te signaleren. De inzichten, inschattingen en verwachtingen die de deskundigen deelden tijdens de kennistafel worden samengevat in Kader 1.

Kader 1. Bevindingen van de kennistafel over achtergrondkenmerken



Deze groep cybercriminelen lijkt overwegend, zelfs bijna uitsluitend, te bestaan uit mannen. Binnen de gemeenschap wordt het als opmerkelijk gezien als een van hen een vrouw blijkt te zijn. In totaal zijn waarschijnlijk tienduizenden personen betrokken bij dit soort cybercrime.

De cybercriminelen zouden over het algemeen tussen de 15 en 50 jaar oud zijn. Vaak zijn ze begonnen tijdens hun studie, meestal tussen de 18 en 23 jaar oud. Hogerop in de organisatie zijn oudere cybercriminelen actief. Veel van de eerste generatie cybercriminelen die actief werden in de jaren 2000 zijn geboren in de jaren '80.

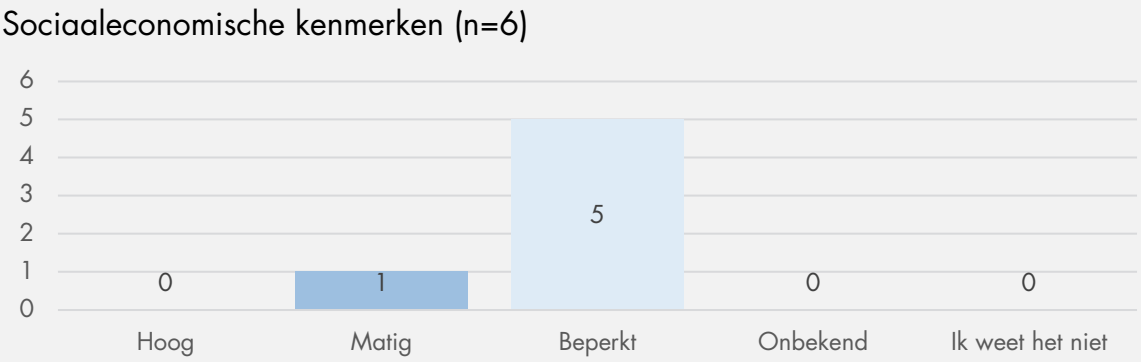
Van de Russischsprekende cybercriminelen is meer dan de helft afkomstig uit Rusland zelf, een kwart uit Oekraïne, en een kwart uit andere landen uit de regio, zoals Moldavië, Kazachstan en de Baltische staten. Om deel te nemen aan ransomware-operaties die we tegenwoordig veel zien is het noodzakelijk om vloeiend Russisch te spreken.

Veel daders lijken afkomstig uit een stedelijke omgeving, zoals Moskou en Sint-Petersburg. Daarnaast zijn er ook clusters van individuen die zich bezighouden met cybercrime in gebieden buiten de grote steden,

met name waar veel geschoolde mensen wonen, in economisch achtergestelde, voormalige Sovjet-industriegebieden.

Leeftijd en nationaliteit kunnen gekoppeld worden aan het soort cybercriminele activiteiten waarmee de individuen zich bezighouden. Zo houden Russische cybercriminelen zich doorgaans meer bezig met ransomware, en zijn Oekraïense cybercriminelen relatief vaker betrokken bij phishing-aanvallen. Phishing is een minder complexe vorm van cybercrime, en om die reden zijn hier relatief meer jongere criminelen bij betrokken. Jongeren fungeren vaker als *initial access brokers*, tussenpersonen die inbreken in systemen en deze toegang vervolgens doorverkopen aan anderen, en zijn actiever in het penetreren van systemen en de uitvoering van aanvallen. Meer ervaren, en dus oudere, cybercriminelen zijn vaker betrokken bij het ontwikkelen en controleren van geavanceerde malware.

De kennis over de demografische kenmerken van deze groep cybercriminelen is vooral opgedaan via opsporing door de politie, gelekte chats, daderinterviews en semi-etnografisch onderzoek. Met name de uitgebreide politiedata geven inzicht in demografische kenmerken. Door de beperkte samenwerking met de Russische autoriteiten, ook vóór de invasie van Oekraïne, hebben opsporingsdata in de meeste gevallen niet geleid tot rechtszaken, bewezen betrokkenheid en veroordelingen. Over andere demografische kenmerken dan geslacht en leeftijd is minder bekend.



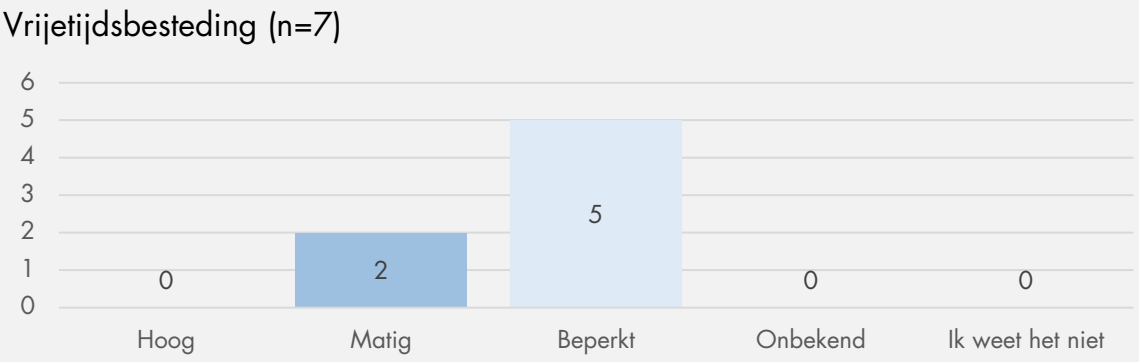
De meeste cybercriminelen binnen deze groep lijken geen welgestelde achtergrond te hebben wanneer ze aan hun cybercriminele carrière beginnen. Een relatief zwakkere economische basis vergroot de financiële motivatie om tot cybercrime over te gaan, die minder speelt bij politiek gemotiveerde criminelen.

Voor zover bekend zijn de cybercriminelen in kwestie vaak hoog opgeleid. Onder de Russische bevolking in het algemeen is het opleidingsniveau hoog: een groot deel gaat naar de universiteit. Een groot deel van de groep cybercriminelen volgt of volgde een studie Informatica of een vergelijkbare opleiding. Anderen hebben zichzelf de benodigde vaardigheden voor het uitvoeren van cybercriminele activiteiten aangeleerd. Vergeleken met het Westen zijn de IT-salarissen in Rusland en Oost-Europa relatief laag. Cybercrime kan aantrekkelijk zijn vanwege het lage risico om gepakt te worden en de grote financiële beloningen die het biedt. Zolang Russische cybercriminelen zich houden aan de patriottische code om geen bedrijven uit Rusland en enkele andere landen uit de voormalige Sovjet-Unie aan te vallen, voelen cybercriminelen zich over het algemeen veilig voor opsporing. Het lijkt niet gebruikelijk voor daders om naast hun cybercriminele activiteiten een reguliere baan te hebben.

Er is geen bewijs dat de cybercriminelen direct gelieerd zijn aan het Russische leger. Via gelekte gegevens zijn beelden bekend van bekende cybercriminelen in militaire uniformen. Door de dienstplicht hebben veel

mannen in Rusland een band met het leger. Daarnaast biedt het leger kansen aan economisch achtergestelde personen, waardoor ze vaardigheden leren die later van pas kunnen komen bij cybercriminele activiteiten. Dit betekent niet direct dat ze in volledige militaire dienst zijn, of dat hun cybercriminele activiteiten verband houden met militaire structuren. Maar cybercrime wordt wel gezien als goed alternatief wanneer ze uit het leger gezet worden, bijvoorbeeld vanwege disciplinaire overtredingen. Er zijn aanwijzingen voor banden met de GRU (de militaire inlichtingendienst van Rusland) evenals de FSB (de federale veiligheidsdienst). Wanneer individuen zich omhoog werken in de hiërarchie van een criminele groep en ze door hun vergaarde rijkdom aandacht naar zich toetrekken, is het aannemelijk dat ze banden proberen aan te gaan met overheidsfunctionarissen om ervoor te zorgen dat ze zaken kunnen blijven doen.

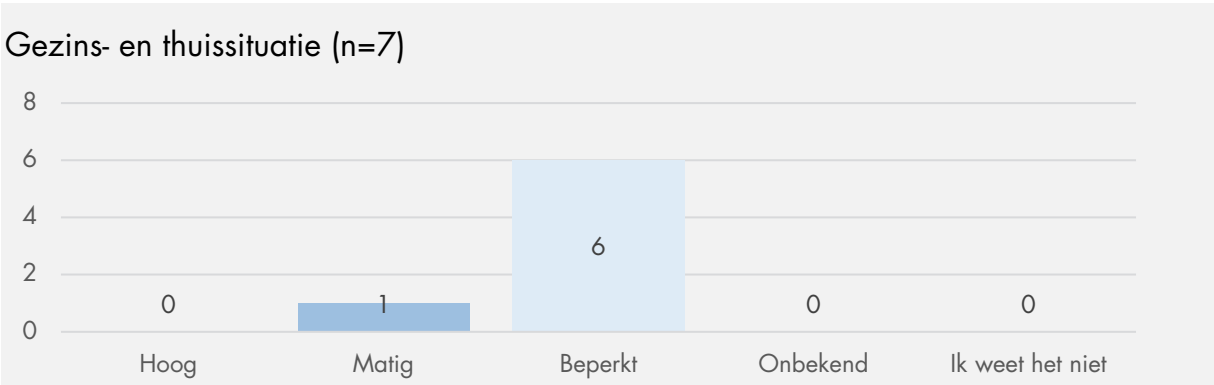
Over de sociaaleconomische kenmerken van deze groep is weinig bekend. Het kan nuttig zijn hier meer over te weten om tot een scherper daderprofiel te komen, maar voor opsporing en preventie zijn sociaaleconomische kenmerken minder relevant.



Cybercriminelen zouden vaak computer-gerelateerde hobby's hebben, zoals gamen. Over het algemeen zouden ze een bovengemiddelde interesse hebben in activiteiten die als 'nerdy' gezien worden. Uit de tienduizenden gelekte interne chatlogs van met name Conti hebben onderzoekers uiteenlopende inzichten opgedaan over het persoonlijk leven van de cyberdaders in kwestie, zoals hun gamenamen, Netflix-voorkeuren en woonplaats. Ook zou deze groep cybercriminelen veel interesse hebben in luxegoederen, met name sportauto's. Sommigen pronken graag met hun rijkdom naar gelang hun sociaaleconomische status, en scheppen op over hun luxueuze vakanties naar Dubai of de Malediven. Maar de groep is divers; anderen binnen dezelfde groep leven een discreter bestaan. Het is mogelijk dat de gelekte chats niet representatief zijn voor de gehele groep cybercriminelen.

Gamen is een mogelijke *gateway* naar cybercrime in het criminele traject van cybercriminelen in het algemeen. Ze beginnen met gamen, maken kennis met het modificeren van spellen, en komen bijvoorbeeld via fora in aanraking met DDoS-aanvallen op andere gamers als vergelding. Als cybercriminelen hierbij betrokken zijn en deze criminelen onder de indruk zijn van hun vaardigheden, kunnen ze worden gerekruteerd.

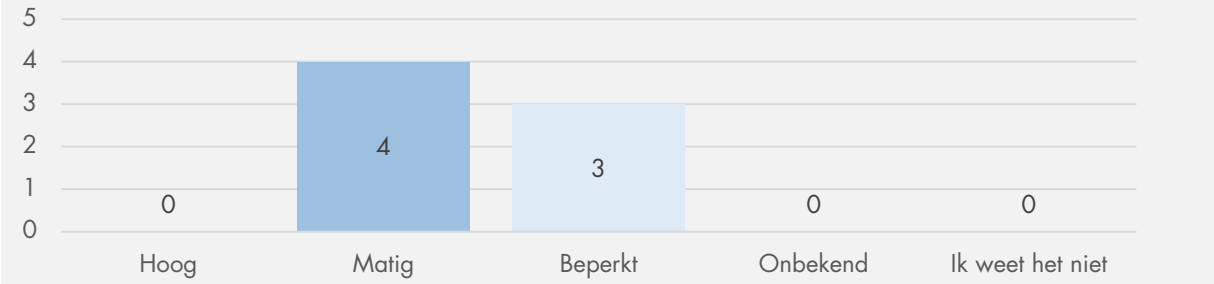
Over de vrijetijdsbesteding van deze groep is vooral anekdotische informatie beschikbaar. Uitgebreidere inzichten op dit vlak, bijvoorbeeld welke games en platforms door cybercriminelen worden gebruikt of wat hun gebruikelijke vakantiebestemmingen zijn, zou opsporing vergemakkelijken.



Rusland heeft veel éénkindgezinnen en een relatief hoog scheidingspercentage. Dit kan van invloed zijn op de thuis- en gezinssituatie van Russische cybercriminelen. Er is geen reden om aan te nemen dat cybercriminelen onevenredig meer of minder uit gebroken gezinnen komen, maar relatief veel huishoudens in Rusland zijn instabiel. Daarnaast hebben ouders mogelijk niet door wat hun kinderen op de computer doen. Tegelijkertijd lijken familiebanden juist beter te zijn dan bij kinderen die betrokken zijn bij 'traditionele' criminaliteit.

Anekdotisch is bekend dat sommige cybercriminelen bij hun ouders woonden en hun cybercriminele activiteiten uitvoerden vanuit het ouderlijk huis. Uit gelekte chats in combinatie met sociale media wordt soms afgeleid dat sommigen van hen een relatie hebben. Ook zijn enkele gevallen bekend van hooggeplaatste cybercriminelen wiens familie hun criminele activiteiten afkeurt. Het lijkt niet gebruikelijk dat cybercriminelen bij hun criminele activiteiten samenwerken met familieleden.

De bewijskracht voor de spaarzame inzichten over de gezins- en thuissituatie van deze groep cybercriminelen is relatief laag. Het is voor onderzoekers lastig dit type bevindingen te verifiëren. Toegang tot deze informatie is nuttig voor het identificeren van factoren die bijdragen aan *desistance*, oftewel het stoppen met het plegen van delicten, zoals een partner die het criminele gedrag afkeurt.



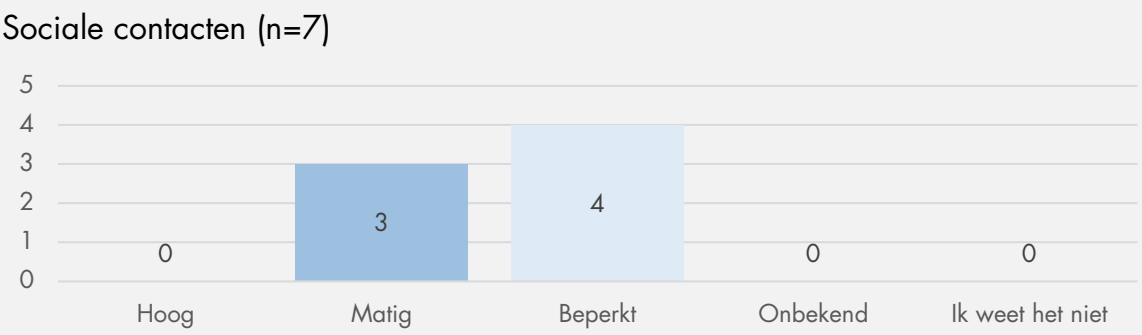
Cybercrime kan een stressvolle bezigheid zijn. De inzet is hoog en er is sprake van een *winner-takes-all*situatie. Dat geldt vooral voor ransomware, waarbij iemand met een succesvolle misdaad in een klap heel rijk kan worden, en een mislukte poging leidt tot reputatiebeschadiging. Er zijn aanwijzingen dat deze groep cybercriminelen soms stress ervaart. In sommige gevallen leidt dit tot het gebruik van drugs, zoals cocaïne en cannabis. Uit interviews met hooggeplaatste cybercriminelen blijkt dat ook zij problemen kunnen hebben met hun geestelijke gezondheid en middelenmisbruik. Maar over het algemeen lijkt dit geen structureel kenmerk van deze groep en zouden ze juist een vrij professionele werkhouding hebben, zoals

geen alcohol drinken tijdens het werk. De leider van Conti, bijvoorbeeld, staat bekend als een nuchter en zeer goed georganiseerd persoon.

Vertrouwensproblemen zouden veel voorkomen bij criminelen. Cybercriminelen zijn in dat opzicht geen uitzondering. Tegelijkertijd is het opvallend dat sommige topcriminelen bereid zijn geweest om de publiciteit te zoeken door interviews te geven. Mogelijk spelen narcisme en de behoefte aan roem en erkenning van hun positie binnen de gemeenschap een rol. Ze voelen zich daar in ieder geval veilig genoeg voor.

Cybercriminelen lijken vaker autisme te hebben. Ze lijken makkelijker online te communiceren dan offline. Voor cybercriminelen lijkt autisme minder tot diskwalificatie te leiden dan voor andere criminelen. Wel lijkt er een verband met de rol die de cybercriminelen vervullen in grotere georganiseerde groepen. Zo werken mensen die autisme hebben eerder als programmeur dan in een rol die sterke communicatieve vaardigheden vereist, zoals een managementfunctie.

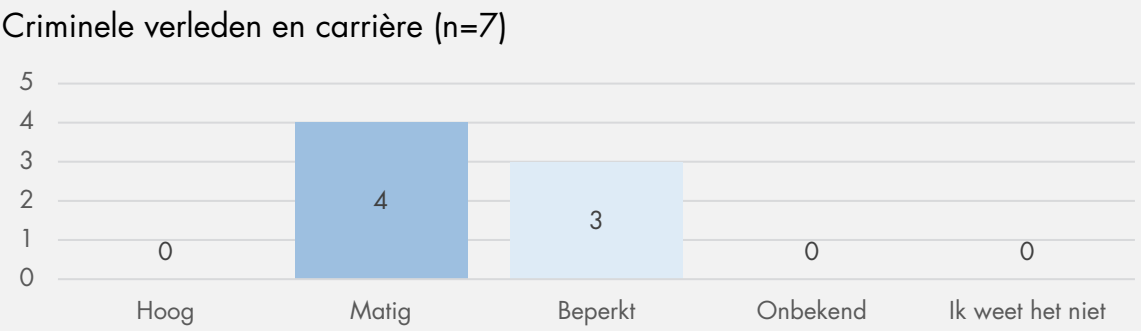
Over psychologische kenmerken is relatief meer en betere informatie beschikbaar dan over sociaaleconomische kenmerken, vrijetijdsbesteding of de thuissituatie. Sommige gegevens die inzichten opleveren over de psychologische kenmerken van de groep als geheel, zijn openbaar beschikbaar. Voorbeelden hiervan zijn arrogantie in de online omgang en de stereotypen die worden gebruikt. Hiervoor is het niet nodig direct de identiteiten van de personen te weten ('pre-attributiegegevens'), in tegenstelling tot enkele andere aspecten. Het is echter lastiger informatie te verkrijgen over hun zelfbeeld.



Persoonlijke ontmoetingen tussen samenwerkende cybercriminelen lijken uitzonderlijk. Hoewel de criminelen binnen een groep aanvallen in samenwerking uitvoeren, soms jarenlang met dezelfde 'collega's', komen ze hiervoor zelden fysiek samen. Vooral de jongere generatie criminelen lijkt elkaar nooit te ontmoeten. In essentie is het dus individueel werk, al zijn er voorbeelden van groepen waar de criminelen elkaar regelmatig persoonlijk ontmoeten in Moskou en Sint-Petersburg, zoals Conti en Wizard Spider. Zij zouden ook met FSB-functionarissen in FSB-gebouwen zijn samengekomen.

Over de sociale contacten buiten de 'werkomgeving' is niet veel informatie beschikbaar. Om persoonlijke relaties niet op het spel te zetten als gevolg van *doxing*, waarbij persoonlijke gegevens worden gepubliceerd, zijn cybercriminelen op hun hoede om persoonlijke informatie te delen. Het is niet duidelijk in hoeverre inzichten over de (beperkte) sociale contacten van cybercriminelen in het algemeen ook van toepassing zijn op de groep in kwestie. Het gedrag en het sociale netwerk van cybercriminelen zou bovendien uiteenlopen tussen verschillende subgroepen, bijvoorbeeld tussen kernleden en jonge, opkomende cybercriminelen. Meer inzicht in sociale contacten zou nuttig zijn voor pogingen om contact te leggen met bepaalde cybercriminelen. Dit maakt meer etnografisch onderzoek mogelijk. Als de bilaterale verhoudingen met Rusland verbeteren, zou betere bereikbaarheid het makkelijker maken om deze

cybercriminelen te laten inzien dat hun criminele gedrag, zowel offline als online, wordt afgekeurd door hun omgeving, en dat er andere mogelijkheden zijn om hun vaardigheden te benutten.



De cybercriminelen lijken geen strafblad te hebben wanneer ze beginnen met cybercrime. Er zijn geen aanwijzingen dat ze duidelijke toekomstplannen hebben, noch de ambitie om grote criminelen te worden. Ook lijken ze zich niet met andersoortige misdaad bezig te houden. Gewelddadige vergeldingen lijken niet voor te komen in de cybercrimewereld. In sommige gevallen hebben ze wapens in hun bezit, maar dit lijkt dan alleen bedoeld voor zelfbescherming wanneer grote hoeveelheden geld in het spel zijn.

Op basis van de beschikbare informatie kan een voorlopig algemeen beeld gevormd worden van het criminele verleden en de carrière van cybercriminelen. Het criminele verleden van een individu is echter lastig te achterhalen, tenzij diegene aan arrestatiegegevens van de lokale politie kan worden gekoppeld. Cybercriminelen hebben echter de neiging op te scheppen over hun prestaties om hun reputatie te versterken. Om lid te kunnen worden van een groep is het bovendien vaak nodig om informatie over criminele activiteiten in het verleden te delen, bijvoorbeeld een bepaalde hack of een gebruikersnaam op een forum. Een belangrijke kanttekening bij de bewijskracht van dit type data is dat de cybercriminelen mogelijk hun criminele verleden en gedeelten van hun criminele carrière verhullen, uitvergroten of erover liegen. Niettemin zijn inzichten in vroegere activiteiten nuttig voor het in kaart brengen van andere achtergrondkenmerken, zoals demografische kenmerken.

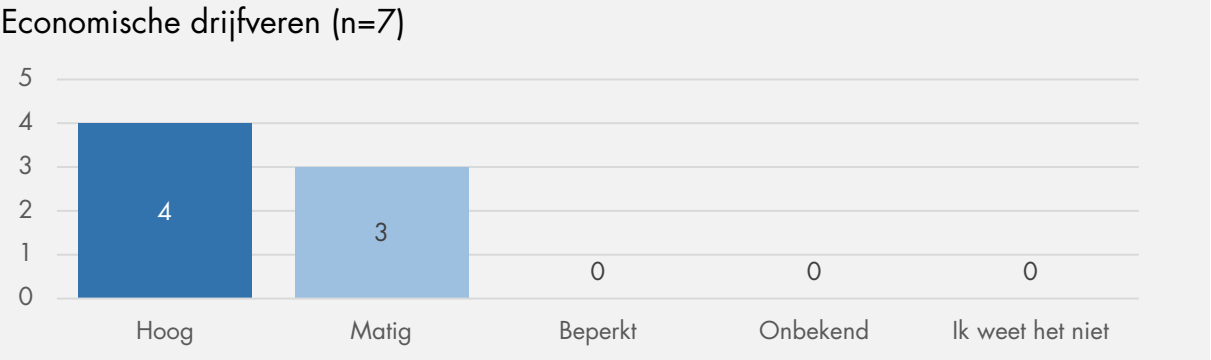
3. Drijfveren

De wereld van cybercrime is toegankelijk, anoniem en dynamisch (Nederveen & Silfversten 2021). Zoals in het vorige hoofdstuk ter sprake gekomen, is het risico om gepakt te worden laag, wat de aantrekkingskracht van cybercrime vergroot. Daderprofielen van cybercriminelen kunnen worden aangescherpt door kennis over de drijfveren (Van der Wagen et al. 2019). Uiteenlopende drijfveren spelen een rol bij cybercriminele activiteiten. Martineau et al. (2023) identificeerden 15 drijfveren in hun systematische review van cyberdaderliteratuur. Wij hebben deze drijfveren, evenals aanvullende drijfveren genoemd in andere bronnen, onderverdeeld in vijf categorieën:

1) Economische drijfveren (financieel gewin en een gebrek aan werkgelegenheid);
2) Sociale drijfveren (beruchtheid, wraak, erkenning door andere cybercriminelen, of om te ontsnappen aan het offline leven);
3) Intellectuele drijfveren (intellectuele uitdaging, prestatiegevoel of nieuwsgierigheid);
4) Psychologische en gedragsmatige drijfveren (verslaving, impulsiviteit en vandalisme); en
5) Politieke drijfveren (ideologische motieven en chantage).

De verschillende drijfveren zijn niet wederzijds uitsluitend. Individuen kunnen gemotiveerd worden door een combinatie van deze factoren. De inzichten, inschattingen en verwachtingen van de deskundigen die zijn gedeeld tijdens de kennistafel worden samengevat in Kader 2.

Kader 2. Bevindingen van de kennistafel over drijfveren



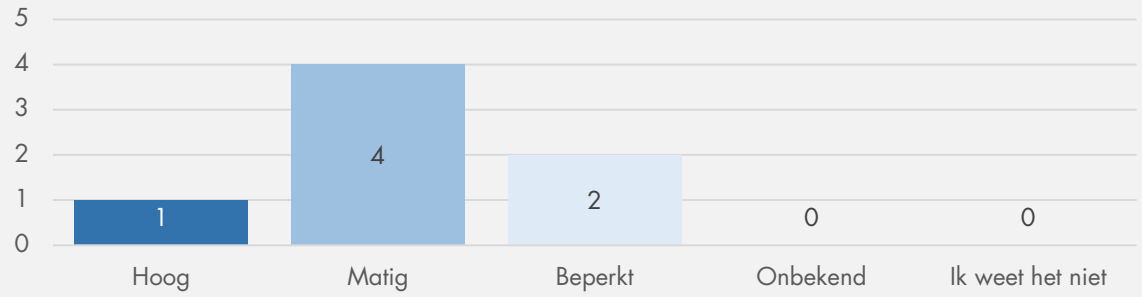
Financieel gewin lijkt een primaire drijfveer voor deze groep cybercriminelen. Er is veel informatie over hoeveel geld wordt verdiend met cybercrime. Bedrijven die slachtoffer zijn van aanvallen maken steeds vaker bekend hoeveel zij aan criminele groepen hebben betaald. Daarnaast blijkt uit het feit dat bijna alle diensten

en vaardigheden tegen betaling worden aangeboden dat financieel gewin een belangrijke drijfveer is. Bovendien is in veel Oost-Europese landen, waaronder Rusland en Oekraïne, weinig sociale zekerheid en betalen IT-banen minder dan in het Westen. Waar personen in West-Europa en Amerika op een legale manier veel geld kunnen verdienen met hun vaardigheden, is dit in Oost-Europa minder het geval. Hierdoor is het snelle, grote geld van cybercrime aanlokkelijker.

Het belang van financiële drijfveren kan naargelang de carrière veranderen. Individuen kunnen in eerste instantie door interesse in IT betrokken raken bij cybercrime, en uiteindelijk geld als grotere drijfveer krijgen. Daarnaast hoeven financiële drijfveren niet doorslaggevend te zijn. Zo werd opgemerkt dat cybercriminelen die al heel veel geld hebben verdiend, toch actief blijven. Dit kan erop wijzen dat andere motieven ook een rol spelen, bijvoorbeeld de wens om de beste te zijn.

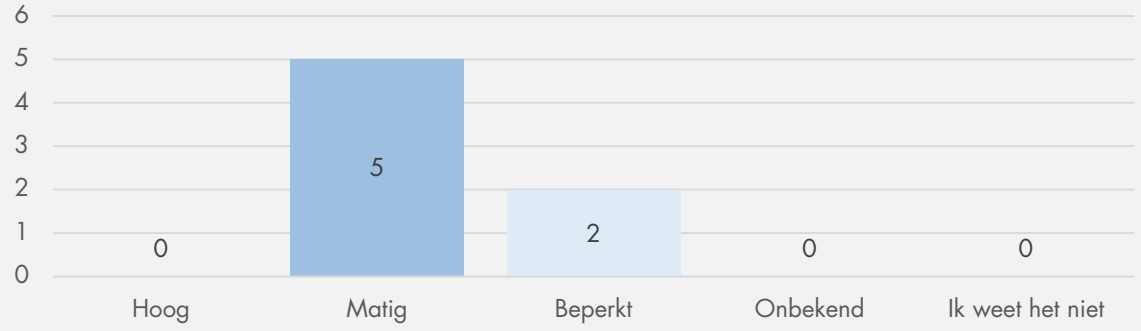
Over economische drijfveren is veel informatie beschikbaar. Hoeveel geld wordt verdiend en hoe dit wordt verdeeld, is uitgebreid gedocumenteerd. In chatgesprekken worden bijvoorbeeld percentages genoemd die verbonden zijn aan specifieke rollen, waardoor inzicht ontstaat in de gemaakte verdeling van het geld dat verdiend wordt. Ook is er een goed beeld van de inkomsten van junior programmeurs. Aangezien losgeld doorgaans via cryptogeld wordt betaald, is er een spoor traceerbaar waaruit mogelijk kan worden afgeleid hoe het geld wordt verdeeld.

Sociale drijfveren (n=7)



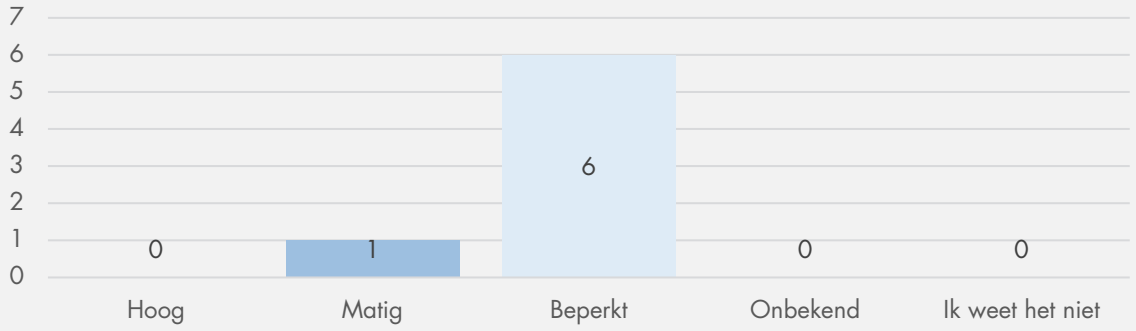
Er is over het algemeen veel bekend over sociale drijfveren op groepsniveau, maar voor specifieke individuen is dit lastiger te achterhalen. Er is anekdotisch bewijs dat elementen zoals prestige en erkenning binnen en buiten de gemeenschap sterke drijfveren kunnen zijn. Ook zijn er aanwijzingen dat cybercriminelen als rolmodel fungeren, met grote invloed op anderen.

Intellectuele drijfveren (n=7)



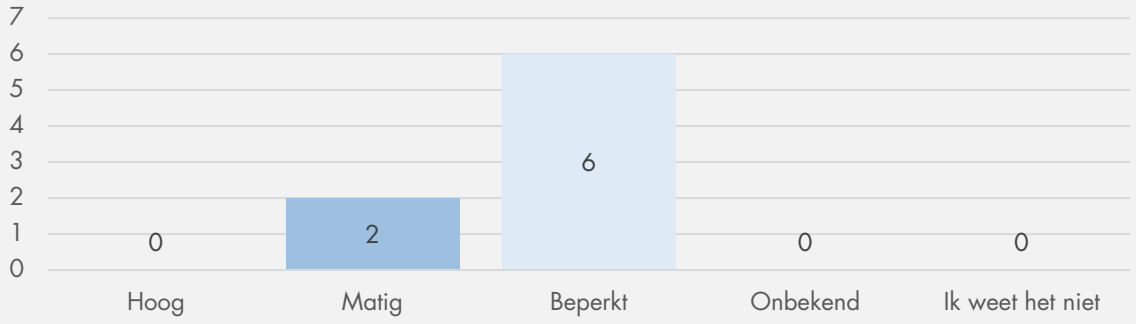
Er is veel inzicht in de kracht van intellectuele drijfveren, maar minder in hoe dit kan worden benut. De intellectuele uitdaging van hacken kan een krachtige drijfveer zijn voor cybercrime. Dit geldt echter eveneens voor ethisch hacken (ook wel *whitehat*-hacken genoemd). Meer inzicht in wat deze uitdagingen aantrekkelijk maken kan helpen om personen uit de criminaliteit te houden en hen ervan te overtuigen hun vaardigheden voor nobelere doelen in te zetten.

Psychologische en gedragsmatige drijfveren (n=7)



Er is beperkte informatie beschikbaar over psychologische en gedragsmatige drijfveren. Deze drijfveren zijn minder zichtbaar, en cybercriminelen zijn hier over het algemeen minder open over. Cybercriminelen kunnen bovendien onbewust door psychologische factoren worden gedreven. Uit gelekte gesprekken of activiteit op sociale media worden wel bepaalde inzichten verworven over hun persoonlijkheid, al geldt dit voornamelijk voor cybercriminelen die erg uitgesproken zijn en de publiciteit zoeken. Er is minder bekend over de mate waarin psychologische en gedragsmatige drijfveren een rol spelen bij cybercriminele activiteiten dan over de psychologische kenmerken en het zelfbeeld van cybercriminelen, zoals besproken in het vorige hoofdstuk.

Politieke drijfveren (n=8)



Politieke drijfveren zijn de laatste jaren zichtbaarder geworden. Het DDoS-hacktivist collectief NoName kondigde in Telegramkanalen aanvallen aan tegen doelwitten in landen die Oekraïne steunen. Andere cybercriminele groepen betuigden steun aan de Russische regering op online fora of het dark web. Steunbetuigingen kunnen gemotiveerd zijn uit de wens gedoogd te worden door de autoriteiten, maar hebben potentieel negatieve gevolgen. Zo werden de chatgesprekken van Conti gelekt door een Oekraïens lid nadat deze groep steun betuigde aan Rusland, wat leidde tot het uiteenvallen van de groep. Politieke drijfveren zijn evident bij hacktivisme en spelen vaak een rol bij DDoS-aanvallen. Daarentegen worden ransomware-groepen bij aanvallen op westerse bedrijven voornamelijk gedreven door opportunisme. De

cybercriminelen zouden het beeld hebben dat westerse bedrijven eerder geneigd zijn het losgeld te betalen dan bijvoorbeeld Aziatische bedrijven.

De cybercriminelen lijken niet altijd een duidelijke politieke oriëntatie te hebben. Over het algemeen spiegelen hun politieke en algemene wereldbeelden die van andere hoogopgeleide Russen die in de grote steden wonen. Uit onderlinge communicatie en datalekken, bijvoorbeeld van de Navalny-beweging, lijken ze de Russische autoriteiten vaker niet dan wel te steunen. Veel cybercriminelen uiten hun ideeën openlijk en steunen de Russische oppositie. Het is onduidelijk hoe deze politieke oriëntatie zich verhoudt tot het eerder gemaakte punt onder sociaaleconomische kenmerken dat de cybercriminelen uit opportunistische overwegingen relaties proberen aan te gaan met overheidsfunctionarissen zodra ze zich omhoog werken in de hiërarchie van een criminele groep.

Anekdotisch zijn er aanwijzingen van communicatie tussen de Russische staat en cybercriminelen. Uit de gelekte Conti-documenten komt naar voren dat de groep op voorhand op de hoogte was van de invasie van Oekraïne in 2022.

Er is beperkte informatie beschikbaar over politieke drijfveren. Bij ransomware-groepen zijn politieke drijfveren moeilijker te identificeren dan bij hacktivistische groepen.

4. Rekrutering

De toeleveringsketen van cybercrime wordt steeds complexer, omdat cybercriminelen zich blijven specialiseren, commercialiseren en samenwerkingsverbanden aangaan voor bepaalde operaties. Voorbeelden van algemene specialisatiegebieden in een cybercriminele groep zijn: kwetsbaarheden identificeren, detectie vermijden, de uitvoering van cyberaanvallen, ondersteuning van de marktplaats, het opnieuw beschikbaar maken van winsten om verdere aanvallen mogelijk te maken, HR en technologische ondersteuning (Huang et al. 2018). Rekrutering voor cybercriminele organisaties kan plaatsvinden via cybercriminele fora, netwerken van gelieerde hackers of op basis van vertrouwen of reputatie. Er is nog weinig literatuur die de rekrutering van cybercriminelen systematisch in kaart brengt, laat staan specifiek voor de groep cybercriminelen uit Oost-Europa die hier centraal staat.

Wij maakten daarom een onderverdeling in drie categorieën:

1) Strategieën en manieren om te werven (o.a. kanalen die worden gebruikt voor werving en de manieren om kandidaten naar deze kanalen te lokken, het eerste contact, de rol van bestaande relaties en sociale netwerken, de mate waarin contacten lokaal verankerd zijn, de rol van reputatie en vertrouwen en hoe groepen zich proberen te onderscheiden als ze uit dezelfde groep rekruteren);
2) De vereiste vaardigheden en ervaring (o.a. de rollen waarvoor groepen proberen te werven, de vaardigheden en expertise die gezocht worden of de informatie waartoe de kandidaten toegang dienen te hebben en hoe vaardigheden en motivatie worden beoordeeld); en
3) De arbeidsomstandigheden en voordelen (o.a. de vergoeding en salarisvoordelen, exclusieve toegang tot middelen of tools, carrièremogelijkheden, opleiding en ontwikkeling, het belang van het sociale aspect van het behoren tot de gemeenschap van de groep, prestatiemanagement en contact).

De bevindingen rondom rekrutering lopen uiteen voor verschillende typen cybercriminelen en cybercriminele groepen. De doelstelling was in de eerste plaats tot een algemeen overzicht te komen van de kennis over de groep als geheel. De inzichten, inschattingen en verwachtingen van de deskundigen die zijn gedeeld tijdens de kennistafel worden samengevat in Kader 3.

Kader 3. Bevindingen van de kennistafel over rekrutering

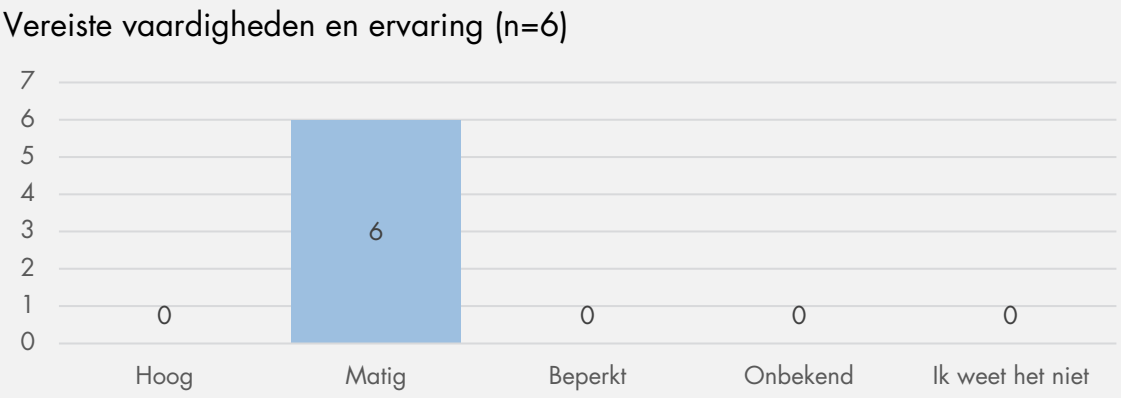
Personeel zou in de eerste plaats worden geworven op online fora. Bekende voorbeelden zijn de fora Xss.is en exploit.in op het dark web. In sommige gevallen zijn formele wervingsprocedures opgetuigd, waar kandidaten hun CV, motivatiebrief, referenties en een overzicht van Bitcoin-portefeuilles moeten aanleveren. Ook worden soms sollicitatiegesprekken gevoerd, bijvoorbeeld via versleutelde chat-applicaties zoals qTox. Het komt voor dat kandidaten bepaalde tests moeten volbrengen om hun vaardigheden te bewijzen, bijvoorbeeld door te tonen dat ze in een bepaalde organisatie kunnen binnendringen. Het lijkt overigens gebruikelijker dat personen hun diensten en expertise zelf aan groepen aanbieden dan dat via vacatures wordt geworven. Bovendien komt het vaak voor dat personen door andere leden binnen de organisatie worden aangedragen.

Cybercriminelen passen verschillende rekruteringstrategieën toe. Cybercriminele groepen maken gebruik van meerdere methoden om handlangers te rekruteren, waaronder het plaatsen van advertenties op legitieme websites voor bepaalde taken zoals programmeren, of het inhuren van diensten via het dark web. Daarnaast kunnen zij ook mensen benaderen die toegang hebben tot gevoelige informatie (zogenoemde *insiders*) binnen organisaties die een doelwit zijn. Het geld dat met cybercrime wordt verdiend, moet vervolgens worden witgewassen. Uit dossiers met betrekking tot de aanklachten tegen Trickbot is veel informatie beschikbaar over de manier waarop zij *money mules* rekruteerden. Zo richtten zij zich specifiek op studenten die toegang hadden tot Amerikaanse bankrekeningen, waar cybercriminelen gebruik van konden maken. De studenten ontvingen hiervoor een vergoeding.

Over strategieën en manieren om te werven zijn veel gegevens openbaar beschikbaar. Veel vindt open en bloot plaats op het *surface web*, het publiek toegankelijke gedeelte van het internet dat wordt geïndexeerd door zoekmachines.

Er bestaat een breed spectrum aan arbeidsconstructies. Sommige groepen, zoals REvil, maken gebruik van een bonussysteem. De gelekte Conti-chats laten zien dat die groep bedrijfsmatig werd gerund, met een HR-afdeling, gespecificeerde arbeidsomstandigheden, salaris en het uitroepen van de 'werknemer van de maand'. Conti wordt in dit opzicht echter gezien als uitzondering. Werken met vaste salarissen is niet gebruikelijk in de cybercriminele wereld; meestal wordt gewerkt op freelancebasis. Er zijn voorbeelden van grootschalige ransomware-operaties waarbij slechts een aantal mensen betrokken waren, die de rest van het werk uitbesteedden. Het uitbesteden van taken wordt als veiliger gezien dan werken in een grote vaste groep, omdat het de risico's verkleint om te worden gepakt. Verlof is meestal alleen weggelegd voor cybercriminelen die een gevestigde, goede reputatie hebben. Kleinere cybercriminelen dienen constant beschikbaar te zijn.

Over de arbeidsomstandigheden en voordelen is minder bekend dan over de werving. De hoge organisatiegraad van Conti lijkt zeer uitzonderlijk; de meeste betrokken cybercriminelen zouden alleen achter een laptop werken in verschillende samenstellingen.



Reputatie lijkt een belangrijk element in rekrutering. Vaak dienen potentiële medewerkers te bewijzen dat zij eerder bij cybercriminele activiteiten betrokken zijn geweest. Daarnaast moet het overzicht van hun Bitcoin-rekening getuigen van hun verdiensten met cybercrime. De gemeenschap is relatief klein en heeft onderling veel (online) contact, waardoor het voor buitenstaanders zonder gemeenschappelijke contacten moeilijk is betrokken te worden. Altijd beschikbaar zijn zou worden gezien als een essentiële eigenschap voor cybercriminelen. Hard werken draagt bovendien bij aan een verbeterde reputatie en waardering.

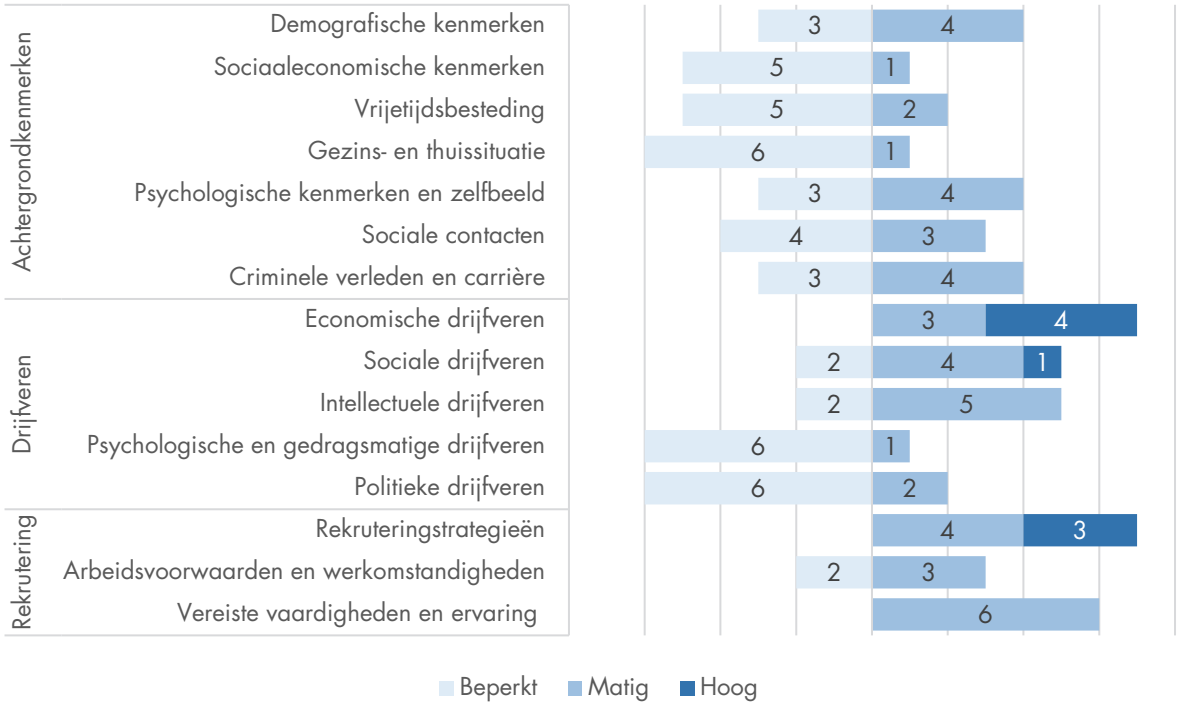
Er is veel informatie beschikbaar over benodigde vaardigheden, maar niet voor zeer gespecialiseerde taken. Zoals hierboven vermeld, zijn uitgebreide vacatureomschrijvingen en wervingsprocedures beschikbaar. Er is daarnaast in het publieke domein veel geschreven over de vereiste vaardigheden en ervaring voor ransomware-activiteiten. Hierdoor is een helder beeld van de persoonlijke vaardigheden en ervaring waar cybercriminele groepen naar zoeken. Zeer gespecialiseerde vaardigheden, bijvoorbeeld niches binnen de cryptografie, zijn echter gewild maar schaars, en vaak niet beschikbaar op cyberfora. Momenteel is niet veel zicht op de rekrutering van personen met deze specialistische vaardigheden voor cyberoperaties.

5. Kennishiaten en toekomstig onderzoek

Cybercriminelen vormen geen homogene groep. De personen die betrokken zijn bij georganiseerde cybercriminaliteit hebben uiteenlopende rollen en profielen. De noodzaak en behoefte aan inzicht over bepaalde typen cybercriminelen kan verschillen voor opsporings- en handhavingsinstanties. Een eerste stap in toekomstig onderzoek naar daderprofielen is het afbakenen van de onderzoeksgroep, en de redenen om meer informatie over hen te vergaren, bijvoorbeeld opsporing, vervolging of preventie.

De dekking en bewijskracht van de beschikbare kennis over de verschillende elementen uit de daderprofielen van cybercriminelen die opereren vanuit Oost-Europa lopen uiteen. Op geen enkel element tasten we compleet in het duister, maar tegelijkertijd is de beschikbare kennis verre van compleet. Dit kan leiden tot een vertekend beeld. De kennis is uitgebreider en sterker wanneer het minder noodzakelijk is om informatie te linken aan de identiteit van specifieke personen (zogenaamde 'pre-attributiegegevens'). Zo is het lastig data te verzamelen over de gezinssituaties, sociaaleconomische achtergrond en psychologische en gedragsmatige drijfveren van de daders, als niet is vastgesteld om welke personen het gaat. Voor aspecten waar dat minder noodzakelijk is, is het eenvoudiger om inzichten te verwerven. Over de vrijetijdsbesteding en de demografische kenmerken van de cyberdaders is bijvoorbeeld veel informatie te verkrijgen, doordat ze hier open over spreken en sporen van achterlaten. Figuur 2 geeft een overzicht van de kennisbeoordelingen van ieder aspect.

Figuur 2. Overzicht van de kennisbeoordeling door de deskundigen



Uit de beoordelingen blijkt het kennisniveau voor drijfveren en rekrutering hoger dan voor achtergrondkenmerken. De deskundigen stellen dat er veel aanwijzingen zijn dat financieel gewin de voornaamste reden is voor cybercrime. Rekrutering vindt relatief openlijk plaats en het is niet altijd noodzakelijk de informatie aan een specifiek individu te verbinden.

De gebieden met het laagste kennisniveau verdienen niet automatisch prioriteit voor toekomstig onderzoek. Evenmin kunnen de gebieden met een hoger kennisniveau terzijde geschoven worden. Een deelnemer stelde dat de gebrekkige kennis over de gezins- en thuissituatie van cybercriminelen geaccepteerd moet worden. Kennis hierover is zeer lastig te achterhalen, en grote investeringen in onderzoek daarnaar wegen niet op tegen de toegevoegde waarde ervan. Het nut van specifieke kennis wordt daarnaast bepaald door externe factoren, bijvoorbeeld de mate waarin samenwerking met lokale autoriteiten mogelijk is. In het geval van Rusland zijn deze mogelijkheden momenteel zeer beperkt.

De deelnemers van de kennistafel vinden wetenschappelijk onderzoek om meer inzicht te krijgen in de volgende aspecten, in willekeurige volgorde, het meest nuttig:

- Het criminele verleden van de cybercriminelen;
- De sociale en psychologische drijfveren die een rol spelen bij technisch onderlegde personen die cybercrimineel worden in plaats van een legaal beroep kiezen in het IT-veld;
- De fora en andere platforms waarop de cybercriminelen actief zijn en de belangrijkste communicatiekanalen die cybercriminelen op een bepaald moment gebruiken;
- Hoe cybercriminelen samenwerken en hun onderlinge rivaliteit;
- De relaties tussen de cybercriminelen en de politiek en ideologische motivaties;

- In hoeverre cybercriminelen samenwerken met inlichtingendiensten en overheidsorganisaties in Rusland en Oekraïne;
- De manieren waarop geld wordt witgewassen.

De vele inzichten over de daderprofielen van cybercriminelen uit Oost-Europa die de deskundigen aan de kennistafel deelden, staan in schril contrast met de beperkt beschikbare academische literatuur. Het zou nuttig zijn als toekomstig onderzoek over de daderprofielen meer primaire data gebruikt. Eerdere literatuurreviews kwamen tot dezelfde conclusie (Bada & Nurse 2021; Leukfeldt & Kleemans 2021; Lusthaus et al. 2023; Martineau et al. 2023). De gegevens die de wethandhavingsdiensten verzamelen, bijvoorbeeld via telefoontaps, IP-taps, observaties, undercover politiewerk en huiszoekingen, leveren welkome complementaire inzichten over de cybercriminelen op. Mogelijk kunnen onderzoekers en politie meer samenwerkingsverbanden aangaan om dergelijke politiedata te benutten. Daarnaast zijn andere primaire bronnen beschikbaar, zoals de gelekte chats, via fora, etnografisch onderzoek en middels kwalitatieve interviews. Martineau et al. (2023) stellen bovendien de noodzaak van meer onderzoek naar hoe cybercriminelen zich op psychologisch, sociologisch, criminologisch en demografisch vlak onderscheiden van zowel niet-cybercriminelen als groepen onderling. Toekomstig onderzoek kan dieper ingaan op de manier waarop bepaalde persoonlijkheidskenmerken gekoppeld zouden kunnen worden aan verschillende rollen binnen de groepen en gemeenschap.

Nader academisch onderzoek kan meer richting geven aan 1) welke kennis het meest nuttig is voor welke doeleinden, zoals preventie of opsporing; 2) hoe cyberdaders in het verlengde daarvan het best geprofileerd kunnen worden; en 3) hoe opgedane kennis over daderprofielen van cybercriminelen in technisch en digitaal forensisch onderzoek geïntegreerd kan worden.

Bronnen

AIVD (Algemene Inlichtingen- en Veiligheidsdienst). 2023. *AIVD Jaarverslag 2022*. Geraadpleegd op 2 april 2024: https://www.aivd.nl/onderwerpen/jaarverslagen/documenten/jaarverslagen/2024/04/22/jaarverslag-2023

Bada, M. & J.R. Nurse. 2021. 'Profiling the cybercriminal: A Systematic Review of Research.' In *2021 International Conference on Cyber Situational Awareness, Data Analytics and Assessment* (CyberSA). IEEE.

CBS (Centraal Bureau voor de Statistiek). 2023. *Cybersecuritymonitor 2022.* Den Haag: Centraal Bureau voor de Statistiek.

Chainanalysis. 2021. 'Eastern Europe's Crypto Crime Landscape: Scams Dominate, Plus Significant Ransomware Activity.' *Chainanalysis*. October 14, 2021.

Cybersecurity and Infrastructure Security Agency (CISA). 2022. '2021 Trends Show Increased Globalized Threat of Ransomware.' 10 februari 2022, Alert CodeAA22-040A. Geraadpleegd op 23 april 2024: https://www.cisa.gov/news-events/cybersecurity-advisories/aa22-040a

Cybersecurity and Infrastructure Security Agency (CISA). 2022. 'Russian State-Sponsored and Criminal Cyber Threats to Critical Infrastructure.' 9 mei 2022, WaarschuwingscodeAA22-110A. Geraadpleegd op 23 april 2024: https://www.cisa.gov/news-events/cybersecurity-advisories/aa22-110a

Felbab-Brown, V. & D. Paz García. 2024. 'Russia, Ukraine, and organized crime and illicit economies in 2024.' Brookings, 6 February 2024. Geraadpleegd op 23 april 2024: https://www.brookings.edu/articles/russia-ukraine-and-organized-crime-and-illicit-economies-in-2024/

Glenny, M. 2023. 'The untold history of today's Russian-speaking hackers.' *Financial Times*, 5 augustus 2023. Geraadpleegd op 23 april 2024: https://www.ft.com/content/9ac188be-8bcf-4b5a-8051-10563683b979

Huang, K., M. Siegel & S. Madnick. 2018. 'Systematically understanding the cyber attack business: A survey'. *ACM Computing Surveys (CSUR)* 51(4): 1–36.

Huisman, W. 2019. 'Levensloopcriminologie, criminele carrières en bijzondere dadergroepen.' *Delikt en Delinkwent* 2019(2): 73-83. Article 2019/6. Geraadpleegd op 23 april 2024: http://deeplinking.kluwer.nl/?param=00D157F9&cpid=WKNL-LTRNav2

International Institute for Strategic Studies (IISS). 2023. '7. Nederland.' In *Cyber Capabilities and National Power*, Volume 2. Geraadpleegd op 23 april 2024: https://www.iiss.org/globalassets/media-library---content--migration/files/research-papers/2023/09/cyber-capabilities-and-national-power-vol-2/cyber-capabilities-and-national-power_volume-2_07-the-netherlands.pdf

Joint Cybersecurity Advisory. 2022. *2021 Trends Show Increased Globalized Threat of Ransomware*.

Leukfeldt, E.R. & E.R. Kleemans. 2021. 'Breaking the Walls of Silence: Analyzing Criminal Investigations to Improve Our Understanding of Cybercrime.' In *Researching Cybercrimes,* edited by A. Lavorgna & T.J. Holt. Palgrave Macmillan, Cham. Geraadpleegd op 13 juni 2024: https://doi.org/10.1007/978-3-030-74837-1_7

Lusthaus, J., E. Kleemans, R. Leukfeldt., M. Levi & T. Holt. 2023. 'Cybercriminal networks in the UK and Beyond: Network structure, criminal cooperation and external interactions.' *Trends in Organized Crime:* 1-24.

Mandiant. 2023. *M-Trends 2023*. Mandiant Special Report.

Martineau, M., E. Spiridon & M. Aiken. 2023. 'A comprehensive framework for cyber behavioral analysis based on a systematic review of cyber profiling literature.' *Forensic Sciences* 3(3): 452-477.

Nationaal Coördinator Terrorismebestrijding en Veiligheid (NCTV). 2023. *Cybersecuritybeeld Nederland 2023.* Geraadpleegd op 23 april 2024: https://www.nctv.nl/documenten/publicaties/2023/07/03/cybersecuritybeeld-nederland-2023

Nederveen, F. & E. Silfversten. 2021. 'Cybercrime activities.' In *Mapping the risk of serious and organised crime infiltration in legitimate businesses*, edited by S. Hulme, E. Disley & E.L. Blondes, 63-67, a145-a160. Luxembourg: Publications Office of the European Union. Geraadpleegd op 23 april 2024: https://op.europa.eu/s/zh2K

Pearce, P. 2018. 'A technical overview of the evidence framework approach: practical ways of thinking about evidence.' *CHESS Working Paper* No. 2018-02, March 2018. [CHESS working paper (Online) 2053-2660].

Peer, W. 2023. 'Waarom zo veel cyberaanvallen uit Oost-Europa komen.' *Algemeen Dagblad*, 11 november 2021. Geraadpleegd op 23 april 2024: https://www.ad.nl/tech/waarom-zo-veel-cyberaanvallen-uit-oost-europa-komen~af2c41fa/

Politie. 2023. *Jaarverantwoording Politie 2022*. Geraadpleegd op 23 april 2024: https://www.politie.nl/binaries/content/assets/politie/onderwerpen/jaarverantwoording/2022/jaarverantwoording-politie-2022.pdf

Privacy-web. 2023. 'Nog meer Nederlandse bedrijven aangevallen door Russische hackers.' 10 augustus 2023. Geraadpleegd op 23 april 2024: https://privacy-web.nl/nieuws/nog-meer-nederlandse-bedrijven-aangevallen-door-russische-hackers

Recorded Future. 2023. 'Dark Covenant 2.0: Cybercrime, the Russian State, and the War in Ukraine.' Geraadpleegd op 23 april 2024: https://go.recordedfuture.com/hubfs/reports/cta-2023-0131.pdf

Silfversten, E., E. Frinking, N. Ryan & M. Favaro. 2019. *Cybersecurity: A State-of-The-Art Review.* Wetenschappelijk Onderzoek- en Documentatiecentrum. Geraadpleegd op 23 april 2024: https://repository.wodc.nl/handle/20.500.12832/2423

United States Department of Justice. 2021. 'Comprehensive Cyber Review.' Geraadpleegd op 23 april 2024: https://www.justice.gov/usdoj-media/dag/media/1232936/dl?inline

Verlaan, D. 2022. 'Woningcorporaties gehackt, ID-bewijzen en bankgegevens op straat.' *RTL Nieuws*, 6 april 2022. Geraadpleegd op 27 mei 2024: https://www.rtl.nl/nieuws/nederland/artikel/5299889/conti-ransomware-cybercriminelen-aanval-woningcorporaties

Van der Wagen, W., E.G. van 't Zand-Kurtovic & T.F.C. Fischer. 2019. *Cyberdaders: uniek profiel, unieke aanpak? Een onderzoek naar kenmerken van en passende interventies voor daders van cybercriminaliteit in enge zin*. WODC Rapport 2974. Geraadpleegd op 23 april 2024: https://repository.wodc.nl/handle/20.500.12832/2432

Zscaler. 2023. *2023 ThreatLabz State of Ransomware*. San Jose, California: ZScaler. Geraadpleegd op 23 april 2024: https://info.zscaler.com/resources-industry-reports-2023-threatlabz-ransomware-report