Towards a new cyber threat actor typology

A hybrid method for the NCSC cyber security assessment

By

Mark de Bruijne, Michel van Eeten, Carlos Hernández Gañán, Wolter Pieters

Faculty of Technology, Policy and Management
Delft University of Technology

Samenvatting

Aanleiding, doel en onderzoeksvragen

Het NCSC/NCTV gebruikt in haar jaarlijkse cyber security beelden een zogenaamde dreigingstypologie—een tabel waarin de dreiging die verschillende actoren vormen in beeld worden gebracht. De cyber actor dreigingstypologie die momenteel gebruikt wordt bestaat al weer enkele jaren en is gedurende deze periode geëvolueerd. NCSC/NCTV vraagt zich af of deze typologie nog steeds valide is, hoe deze zich verhoudt tot recente inzichten uit theorie en praktijk en hoe deze eventueel verbeterd kan worden. Dit rapport, geschreven in opdracht van het WODC van het Ministerie van Veiligheid en Justitie, ontwerpt een nieuwe systematische methodiek die moet leiden tot een verbeterde cyber actor dreigingstypologie.

Om aan dit doel—een nieuwe methodiek voor de ontwikkeling van een nieuwe typologie—te bereiken ontwikkelt het rapport twee producten die in elkaars verlengde liggen. Allereerst wordt de nieuwe methodiek om een cyber actor dreigingstypologie te ontwikkelen beschreven. De methode is gebaseerd op state-of-the-art inzichten in cyber actor typologieën en bevat een gestructureerde werkwijze om cyber actor groepen te classificeren. Net als de jaarlijkse cyber security beelden, beperkt het onderzoek zich tot een cyber actor dreigingstypologie die actor groepen beschrijft die “de betrouwbaarheid en de beveiliging van informatie(systemen)” in Nederland aantasten (NCSC, 2016:21).

Ten tweede wordt op basis van de nieuwe voorgestelde methodiek een eerste versie van nieuwe typologie ontwikkeld op basis van empirische data en dreigingsinformatie over cyber incidenten en cyber actoren uit het Cybersecuritybeeld Nederland (CSBN 2016)(NCSC, 2016). Het onderzoek beoogt nadrukkelijk niet een compleet nieuwe typologie te ontwikkelen die direct gebruikt kan worden. Het rapport illustreert de werking van de nieuwe methodiek. Doel van het rapport is om dreigingsanalisten en experts in het cybersecurity domein een transparante, systematische en repliceerbare methodiek aan te reiken die hen in staat stelt een dynamische cyber actor dreigingstypologie op te stellen. De methode dient gebaseerd te zijn op de meest recente inzichten over typologieën in literatuur rond cyber security, data over veiligheidsincidenten en zodoende een bruikbaar uitgangspunt vormen voor dreigingsanalyses. De methode moet analisten en cyber security practitioners op een transparante maar gestructureerde wijze in staat stellen om inzicht te verkrijgen in welke actorgroepen een dreiging vormen voor de betrouwbaarheid en de beveiliging van informatie(systemen) in Nederland. De onderzoeksvragen die in het onderzoek centraal staan zijn:

1. In welke mate wordt de bestaande cyber actor dreigingstypologie gevalideerd door recente inzichten vanuit de wetenschap en de praktijk en welke ontwerpcriteria voor een verbeterde cyber actor dreigingstypologie kunnen worden geïdentificeerd?

2. Welke methode voor het ontwerpen van een cyber actor dreigingstypologie voldoet aan de geïdentificeerde ontwerpcriteria en verbeterd de huidige cyber actor typologie?

3. Op welke wijze kan een cyber actor typologie worden geconstrueerd die gebaseerd is op state-of-the-art kennis en empirische data over cyber incidenten, en hoe zou zo'n typologie eruit zien?

Onderzoeksopzet

Teneinde een antwoord te genereren op de onderzoeksvragen beschrijft dit onderzoeksproject de ontwikkeling van een nieuwe cyber actor dreigingstypologie. Als startpunt voor de ontwikkeling van de nieuwe methode om een cyber actor typologie te genereren, wordt eerst het concept 'typologie' gedefinieerd. Een typologie is een specifieke classificatiewijze die de gebruiker in staat stelt op een bondige maar gestructureerde wijze geobserveerde patronen te classificeren. Typologieën kunnen gedefinieerd worden als een "verzameling conceptueel afgeleide onderling samenhangende ideaaltypen" (Doty & Glick, 1994:232).

Vervolgens wordt het doel dat met een dreigingstypologie wordt beoogt, en de daarbij behorende ontwerpcriteria nader geanalyseerd. Het doel van de typologie kan worden gevonden in de jaarlijks verschijnende Cybersecuritybeelden. De cyber actor dreigingstypologie stelt analisten in staat om een (nationaal) dreigingsbeeld op te stellen, meer in het bijzonder van "actoren die de betrouwbaarheid en de beveiliging van [Nederlandse] informatie(systemen)(NCSC, 2016:25)" bedreigen. De bestaande cyber actor dreigingstypologie in het Cybersecurity Beeld stamt uit 2011 en is in 2012 aangepast en onderscheidt in haar huidige vorm 9 verschillende actor groepen die een bedreiging (kunnen) vormen. De huidige typologie heeft de volgende tekortkomingen en zwakheden:

1. De typologieën identificeren een intuïtief logische set van actor typen, maar de typologie lijkt niet systematisch opgebouwd. Nadere analyse wijst echter uit dat de typologie niet systematisch is samengesteld. Onduidelijk is welke dimensies in de typologie een rol spelen en hoe tot de classificatie van cyber actor groepen is gekomen.

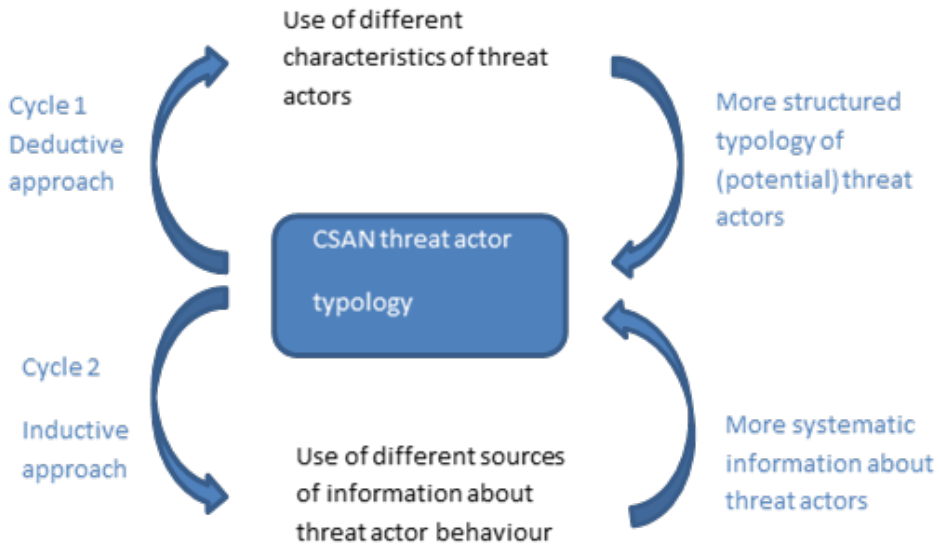
2. De huidige dreigingstypologie is statisch en is niet goed in staat om met verandering en dynamiek om te gaan, terwijl dit nu juist een wezenskenmerk van een typologie is; een systematische procedure om de dreigingstypologie te evalueren en te herzien ontbreekt.

3. De bestaande typologie ontbeert een mechanisme waardoor gebruik wordt gemaakt van de toenemende hoeveelheid en variëteit empirische data die over cyber incidenten, trends en cyber actoren wordt verzameld waardoor de analytische meerwaarde van de typologie voor dreigingsanalyses afneemt. Een gestructureerd proces van data-analyse is noodzakelijk om de relevante trends en ontwikkelingen die via empirische data wordt verzameld te analyseren en te koppelen aan de op systematische wijze verkregen set van actor dimensies.

Een nieuw te ontwikkelen typologie dient tenminste deze tekortkomingen te adresseren. Daarenboven kunnen op basis van literatuur over typologieën een aantal kwaliteitscriteria van een goede typologie worden onderscheiden. In totaal worden via deze analyse vier methodische en vier meer praktische ontwerpcriteria onderscheiden. De methode die leidt tot de nieuwe cyber actor dreigingstypologie dient op een beredeneerde wijze een balans te vinden tussen de geïdentificeerde ontwerpcriteria.

De ontwerpmethode voor een nieuwe typologie

Om te komen tot een ontwerp voor een nieuwe, systematische methode voor de ontwikkeling van een verbeterde cyber actor dreigingstypologie wordt een gecombineerd hybride deductieve en inductieve aanpak beschreven. De methode kent een cyclisch karakter die een continue aanpassing en verbetering van de cyber actor dreigingstypologie mogelijk maakt (cf. Bailey, 1994:3). Dit betekent dat eerst een conceptuele classificatie van actor typen wordt afgeleid uit de literatuur en dat vervolgens empirische data wordt gebruikt om de cyber actor dreigingstypologie te valideren en zo nodig aan te vullen. Figuur 1 beschrijft de methodiek die het best aan de hand van de huidige cyber actor dreigingstypologie in kaart kan worden gebracht. Het rapport beoogt niet om te komen tot een compleet ontwikkelde cyber actor dreigingstypologie; in plaats daarvan beschrijft het rapport de eerste volledige cyclus van de ontwerpmethode die zal moeten leiden tot een nieuwe cyber actor dreigingstypologie. Het rapport en de methode die in het rapport beschreven worden zijn expliciet ontworpen om in de dagelijkse praktijk gebruikt en toegepast te worden door dreigingsanalisten en andere cybersecurity practitioners en continu bij te dragen aan de verbetering van de huidige Nederlandse cyber actor dreigingstypologie.



Figuur 1: Een hybride ontwerpmethode voor een nieuwe cyber actor dreigingstypologie

Cyclus 1: deductieve aanpak

In de eerste ontwikkelcyclus wordt een gestructureerd model van cyber actoren ontwikkeld die een (potentiele) dreiging kunnen vormen voor Nederlandse data systemen. Als startpunt, wordt een beperkt literatuuronderzoek uitgevoerd om dimensies te identificeren die worden gebruikt in (cyber) actor dreigingstypologieën. Google Scholar en (academische) databases Elsevier Scopus en IEEE Xplore werd literatuur doorzocht op zoek naar literatuur over (de ontwikkeling van) een cyber actor dreigingstypologie. Een set zoektermen leverde een 70-tal publicaties op die potentieel relevant materiaal opleverden voor de ontwikkeling van een theoretisch afgeleide cyber actor dreigingstypologie.

De hoofdconclusie van het literatuuronderzoek was dat geen bondige, alomvattende cyber actor dreigingstypologie bestaat en dat veel bronnen onduidelijk zijn over de onderliggende methodiek die ten grondslag ligt aan de ontwikkelde typologieën die wel worden beschreven. Desondanks kon een gedeelde set van karakteristieken worden afgeleid uit de bestudeerde typologieën. Vijf kerndimensies werden geïdentificeerd: ‘doelwit’, ‘expertise’, ‘hulpbronnen’, ‘organisatie’, en ‘motivatie’. Deze kerndimensies worden echter onvolledig en/of onduidelijk geconceptualiseerd en geoperationaliseerd waardoor ze onbruikbaar zijn om cyber actor types te identificeren ten behoeve van dreigingsanalyses.

Een noodzakelijke tweede stap in de deductieve cyclus is de conceptualisatie en operationalisatie van de kerndimensies. Nadat de vijf dimensies van de typologie zijn geoperationaliseerd is het theoretische vraagstuk opgelost. De vijf kerndimensies en de daaropvolgende operationalisatie van de schalen determineren de hoeveelheid te identificeren cyber actor typen in het kader van een dreigingsanalyse. Echter, de hoeveelheid potentiele actor typen conflicteert al snel met de toepasbaarheid en bruikbaarheid van de typologie.

Om informatieanalisten en practitioners te ondersteunen in het terugdringen van de potentiele hoeveelheid cyber actor types wordt een intermediair product opgesteld dat als instrument kan worden gebruikt om het classificatie proces te structureren. Het zogenoemde cyber actor typologie framework bestaat uit een beperkte set vragen die de analisten in staat stelt veiligheidsincidenten of aanvalsscenario’s te classificeren en te koppelen aan de karakteristieken van een (of meerder) potentiële cyber actor typen die deze dreiging veroorzaken. De classificatieschalen en het typologie framework zijn ter validatie voorgelegd aan de 18 respondenten – experts op het gebied van de dreigingsmatrix en internetveiligheid in brede zin. Op basis van de feedback door de respondenten zijn zowel de schalen als het typologie framework aangepast. Op 23 februari 2017 werd tijdens een workshop een finale versie van het cyber actor typologie framework getest. Net als de typologie claimen de onderzoekers ook voor wat betreft het ontwikkelde framework sprake is van een eerste versie. Het framework is als aparte deliverable direct bijgevoegd bij de rapportage en vormt een integraal onderdeel van de ontwikkelde methode voor de ontwikkeling van een nieuwe cyber actor dreigingstypologie.

Cyclus 2: inductieve aanpak

De inductieve aanpak vormt een tweede parallelle stap in de ontwikkeling van de methode om een dreigingstypologie te ontwikkelen. Door empirische data op een systematische wijze te analyseren op de kerndimensies kan gezocht worden naar data die de typologie en kennis van de cyber actor typen en hun werkwijzen kan verbeteren. Hiertoe kan gebruik worden gemaakt van data over specifieke incidenten, internetdata, studies van slachtoffers, interviews met experts, etc. Empirische data kan op deze wijze worden gebruikt om de actor typologie te voeden. In dit onderzoek wordt data van cyber criminele markten, honeypot data, sinkhole data, Darknet/IDS gebruikt om ontwikkelingen en trends te analyseren en te relateren aan de kerndimensies en het gedrag van de actor groepen. Op deze wijze levert de empirische data nieuwe informatie aan kan worden gebruikt om de typologie te ‘voeden’ en de afgeleide deductieve typologie continu up-to-date te houden en continu te verbeteren.

Resultaat: De cirkel gesloten en een eerste aanzet tot een nieuwe cyber actor dreigingstypologie

De twee beschreven cycli creëren de bouwstenen voor de ontwikkeling van de nieuw cyber actor dreigingstypologie: de derde stap van de methode. Uit de deductieve cyclus wordt de cyber actor typologie framework gebruikt. Dit framework wordt gevoed met de informatie uit

de inductieve cyclus en de informatie van grofweg 50 verschillende trends, kwetsbaarheden, aanvallen en aanvalsscenario's die in het Cybersecuritybeeld 2016 worden geïdentificeerd.

Met behulp van een tussenstap worden de verschillende incidenten en trends gecategoriseerd op basis van de kerndimensie motief. Uiteindelijk kan op basis van de beschikbare data over incidenten en trends uit het cybersecuritybeeld een 11-tal cyber actor typen worden onderscheiden: extortionists, information brokers, crime facilitators, digital robbers, scammers and fraudsters, crackers, insiders, terrorists, hacktivists, state actors en state-sponsored networks. Voor elk actor type en elk (verondersteld) aanvalsscenario werd de framework typologie gebruikt om de dreiging te koppelen aan een cyber actor type. Het onderzoek heeft voor deze eerste typologie gebruik gemaakt van de (gelimiteerd) beschikbare informatie uit het Cybersecuritybeeld 2016. De plot is beschreven in Tabel 2.

Door de gestructureerde toepassing van de in dit rapport ontwikkelde methodiek ontstaat een cyber actor dreigingstypologie die significant afwijkt van de typologieën uit de cybersecuritybeelden 2015 en 2016. Tabel 1 geen de belangrijkste verschillen weer.

CSAN actor typology	TU Delft threat actor typology
professional criminals	extortionists information brokers crime facilitators digital robbers scammers and fraudsters
hacktivists	hacktivists
script kiddies	crackers
terrorists	terrorists
state actors	state actors state sponsored network
	insiders
private organizations	
cyber researchers	
'no actor'	

Tabel 1: CSAN 2016 typology and new threat actor typology compared

Veel zo niet alle actor typen uit de dreigingsbeelden lijken ingedeeld te kunnen worden in de nieuwe typologie. In veel gevallen zijn de actor typen te herkennen. In andere gevallen zijn de typen samengevoegd tot een nieuw actor type. De verschillende actor typen kunne geclusterd worden op basis van de kerndimensie motivatie.

De sterk heterogene actor type 'professional criminals' uit de cybersecuritybeelden die een economische motivatie voor hun aanvallen delen valt uiteen in verschillende (sub)actor typen die classificatie op basis van het type aanval vergemakkelijken en leiden tot een meer focus in de beschrijving van de verschillende actor groepen.

Ten tweede wordt het actor type 'state actors' gesplitst. De nieuwe actor typen zijn beiden geopolitiek gemotiveerd. Maar naast het traditionele state actor type dat zich richt op (klassieke vormen van) spionage kan een tweede actor groep worden geïdentificeerd dat gebruik maakt van andere aanvalsvormen maar bovenal anders georganiseerd lijkt. De organisatorische constellatie vertoont kenmerken van een netwerk en bestaat uit meerdere actoren.

The actor typen 'terrorists', 'cyber vandals and script kiddies' en 'hacktivists' die in het dreigingsbeeld werden onderscheiden zijn in de nieuwe typologie samengevoegd en/of

hernoemd. Wat deze heterogene groep van actor typen bindt zijn de motieven. De motieven zijn niet-economisch.

De actor typen ‘cyber vandals’ en ‘script kiddies’ zijn samengesmolten in het actor type ‘crackers’ die een persoonlijke motivatie hebben om aanvallen uit te voeren (bijvoorbeeld: voor de lol of vanwege de reputatie). ‘Crackers’ met verschillende expertiseniveau’s worden onderscheiden, maar de overeenkomst is dat beide subgroepen binnen het actor type niet beschikken over hulpmiddelen om hun aanval te ondersteunen.

‘Terrorists’ en ‘hacktivists’ zijn ook in de nieuwe typologie te herkennen, maar er wordt een strikter onderscheid tussen beide groepen aangehouden. Beide actor groepen delen een ideologische motivatie die ten grondslag ligt aan de aanval, en wanneer het gedrag van de actor typen wordt geanalyseerd met behulp van het typologie framework verschilt dat niet wezenlijk van elkaar. De beide actor groepen verschillen wel als het gaat om de keuze van het doelwit en ook de impact die met de aanval wordt beoogd. Vergeleken met ‘hacktivists’ zijn ‘terrorists’ erop uit om met hun aanval maximale maatschappelijke impact te genereren. Hierdoor zijn aanvallen door deze actor groep erop gericht om maximale schade en/of een maximaal aantal slachtoffers te veroorzaken. Deze karakteristiek is niet als een kerndimensie in de voorgestelde typologie opgenomen. Maar vanwege het onderscheid dat kan worden gemaakt in type aanval en vanwege de latente dreiging van de actor groep wordt het actor type ‘terrorists’ alvast gereserveerd voor zeer destructieve aanvallen. Er bestaat echter nog geen data om dit actor type en de specifieke karakteristieken behorend bij dit actor type in een dreigingsanalyse scherper uit te werken. Het actor type wordt ‘voorspeld’ bij afwezigheid van data om het bestaan van dit actor type te bewijzen.

Het actor type ‘insider’ blijft bestaan, zij het dat de beschrijving van een ‘insider’ wordt aangescherpt. Hulp die ‘insiders’ bieden bij aanvallen uit economisch perspectief wordt meegenomen in de kill chain van andere aanvallen door andere actor typen. Daarmee zijn ‘insiders’ nu individuen die uit persoonlijke motivatie een aanval plegen.

Tot slot verdwijnen drie actor typen: ‘cyber researchers’, ‘private organizations’ en ‘no actor’. De afwezigheid van deze actor typen kan verklaard worden. Allereerst worden ‘private organizations’ als actor type in de nieuwe typologie opgenomen in de verschillende actor types die een hogere organisatiegraad en een financiële motivatie kennen. ‘Cyber researchers’ zijn niet noodzakelijkerwijs direct betrokken bij een aanval en vormen geen onderdeel van de kill chain van veel aanvallen. De financiële motivatie die ten grondslag ligt aan de bijdrage die onderzoekers leveren doet niets af aan het gegeven dat de onderzoeker geen directe aanvaller is. Als de ‘hacker’ of ‘cyber researcher’ daarentegen wel een actieve bijdrage levert aan de kill chain, is sprake van betrokkenheid bij de aanval en zal de ‘cyber researcher’ onderdeel gaan uitmaken van de kill chain van de actor die de aanval uitvoert. Bijvoorbeeld omdat een ‘hacker’ of ‘cyber researcher’ actief een exploit distribueert (verkoopt) aan een klant (een crimineel of een overheid). Door deze redeneerwijze verdwijnt het onderscheid tussen grey en black market ‘cyber researchers’ en grey en black ‘hackers’. Een voorbeeld dat het cruciale onderscheid weergeeft in de rol van de ‘cyber researcher’ vormt de casus van de ‘Hacking Group’.

Het derde actor type is de ‘no actor’ groep. Dit actor type heeft geen plaats in een cyber actor dreigingstypologie. Dat betekent niet dat de onderzoekers security incidenten zonder duidelijk aanwijsbare dadergroep irrelevant vinden of onbelangrijk vinden als bron van kwetsbaarheden. Maar er kan geen sprake zijn van een dreigingsanalyse en de incidenten spelen geen rol in de totstandkoming van een cyber actor dreigingstypologie. In plaats van het actor type ‘no actor’ onderscheidt de nieuwe typologie de dimensie ‘unintentional’, die wijst op onverwachte dreigingen en het falen van beveiligingsmaatregelen. Maar de toepassing van niet-intentionele motieven in de cyber actor dreigingstypologie betekent een

complexe vertaalslag in termen van duiding van incidenten en scenario's die weinig meerwaarde lijkt te genereren. Daarom wordt een incident dat scoort op de schaal 'unintentional actions' uit de framework typologie niet gekoppeld aan een specifiek actor type.

Het onderzoek stelde zichzelf ten doel om de cyber actor dreigingstypologieën die in de cybersecuritybeelden 2011-2016 werden gepresenteerd te verbeteren. Een nieuwe methode is ontwikkeld om te komen tot een verbeterde cyber actor dreigingstypologie. De gepresenteerde cyber actor typologie is echter nadrukkelijk niet bedoeld om gebruikt te worden als een definitieve versie in toekomstig onderzoek; het is een eerste versie van een typologie die pas een volledige ontwikkelcyclus heeft doorlopen. De typologie is gebaseerd op beperkte data. Continue validatie en ontwikkeling van de gepresenteerde cyber actor dreigingstypologie op basis van de voorgestelde methode wordt dan ook van harte aanbevolen.

	Threat actor type	extortionists	information brokers	crime facilitators	digital robbers	scammers and fraudsters	crackers	insiders	terrorists	hacktivists	state actors	state-sponsored networks
Target	Citizens	■	■	■	■	■						
	Enterprises	■	■	■	■	■	■	■	■	■	■	■
	Public Sector	■	■	■		■	■	■	■	■	■	■
	Critical Infrastructure(s)						■		■	■	■	■
Expertise	Low	■				■	■			■		
	Medium	■	■	■	■	■	■	■		■	■	■
	High		■	■	■			■	■		■	■
Resources	Low	■	■			■	■	■		■		
	Medium	■	■	■	■	■			■	■	■	■
	High				■				■		■	■
Organization	Individual					■	■	■		■		
	Hierarchy	■	■						■		■	
	Market	■	■	■		■			■			
	Network	■	■	■	■	■	■			■		■
	Collective						■			■		
Motivation	Personal	■					■	■				
	Economic	■	■	■	■	■		■				
	Ideological							■	■	■		
	Geo-political										■	■

Tabel 2: Threat actor typologie gebaseerd op Cybersecuritybeeld (CSBN) 2016