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

Summary

Reason, purpose and research questions

For some years, the NCSC/NCTV has been using a cyber threat actor typology in its annual Cyber Security Assessment Netherlands (CSAN)—a table that intuitively captures a set of actors with different motives, intentions and capabilities which might threaten the security of the Dutch IT infrastructure. It has evolved over time and. In view of its age and rather intuitive development process, the NCSC/NCTV is considering whether the current typology needs to be updated and improved in light of recent insights from science and cybersecurity practice. This report, which was commissioned by the WODC (Research and Documentation Centre) of the Ministry of Security and Justice, sets out to develop a new and systematic method to enable NCSC/NCTV to continuously update its cyber threat actor typology.

This research develops two distinctive products to fill the knowledge gap. First of all, a new method to develop a threat actor typology is constructed. The method is based upon state-of-the-art insights in cyber actor typologies and features a structured way to classify threat actors. In line with the CSAN, our assignment was to restrict the threat actor typology to the description of actors who either operate from the Netherlands or attack targets in the Netherlands.

Second, the research aims to develop a new tentative threat actor typology from the events, threat intelligence, and data that were reported in the 2016 CSAN. The report shows how the method can be used to include input from diverse data sources about cyber attacks. The researchers do not claim to present a completely new threat actor typology, nor to have drawn up a final version. Rather, the principal aim of this report is to provide threat intelligence analysts and security practitioners with a transparent, systematic and repeatable method to develop the cyber actor typology on an ongoing basis. The research questions which accompany the project goals were:

1. To what extent is the current cyber actor typology validated by recent insights from science and cyber security practice and what design criteria for a new cyber actor typology can be identified?

2. What method to develop a cyber actor typology satisfies the identified design criteria and enhances or enriches the current cyber actor typology different cyber actors?

3. To what extent can a typology be constructed based upon state-of-the art knowledge on cyber actors and empirical data on cyber incidents, and what would the resulting typology look like?

Research approach

In response to the research questions this research project describes the development of a new cyber actor typology. As a starting point for the development of the new method to generate a cyber actor typology, this report first defines the concept ‘typology’. A typology is a specific form of classification that promises to yield a concise yet parsimonious framework to describe and classify observed patterns. Typologies can thus be defined as “conceptually derived interrelated sets of ideal types” (Doty & Glick, 1994:232).

Next the intended use of this cyber actor typology in the annual Cyber Security Assessment Netherlands (CSAN) is identified. This is necessary to align what the final products—the method and the resulting cyber actor typology—actually need to 'do'. The threat actor typology is intended to create a framework of dimensions and classifications that enables a reliable and speedy identification and classification of threat actors and the resulting threat actor landscape that "adversely affect the reliability and security of information and information systems in The Netherlands" (NCSC, 2016:25).

After having identified and articulated the intended use of the desired cyber threat actor typology, and its design requirements, it is time to consider the typology which NCSC/NCTV uses in its annual Cyber Security Assessment Netherlands (CSAN). The cyber actor typology was developed in 2011 and identified 6 cyber actor types and was later extended into 9 cyber actor types in the 2012 CSAN. Three major shortcomings and weaknesses of these typologies are identified:

1. The typologies identify a set of threat actors that makes intuitive sense, but underneath the typology, a variety of dimensions are implicitly at work in an unsystematic way. Consequently, there is unclarity about scientific underpinning of the choice of the dimensions, what role they play and how they affect the classification process and thereby affect the typology.

2. Typologies need to be reviewed periodically, but the CSAN typologies lack a methodology to adjust to developments and are ill-equipped to cope with dynamics.

3. CSAN typologies lack a mechanism to take advantage of ongoing measurement data generated all over the landscape, which erodes the analytic power of the typology for threat assessment. A structured process is needed to capture relevant trends observed in measurement data and map them onto a systematic set of actor dimensions.

Any new method that would result in the development of a cyber threat actor typology would have to address and preferably solve these shortcomings. Furthermore 8 quality criteria for a good typology were identified: 4 methodological and 4 more based upon the intended goals. The new threat actor typology design method would have to strike a motivated balance between these criteria.

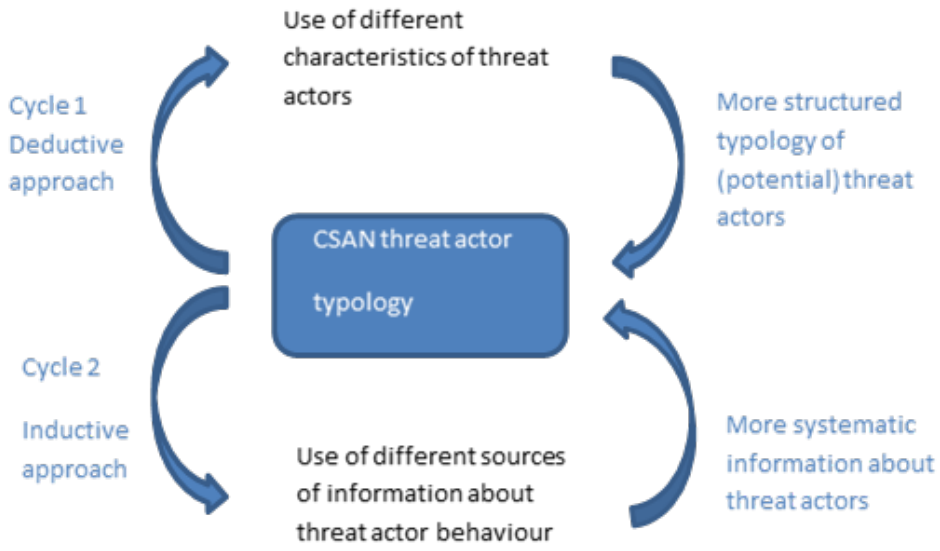

Figure 1: A hybrid method to develop a new threat actor typology

The method to develop a typology

The new method which is proposed to fulfil these criteria and to allow for the creation of a valid and useable cyber threat actor typology is based on a combined 'deductive' and 'inductive' approach, which is cyclical in nature and supports an ongoing, incremental development and improvement of the CSAN cyber threat actor typology—a hybrid approach (cf. Bailey, 1994:3). This means that first, a conceptual classification of threat actors is deduced from literature and secondly, empirical data are used to stimulate so-called induction of the threat actor typology. Figure 1 shows the resulting methodology that is best visualized around the cyber actor typologies that are in use by NCSC/NCTV in the CSAN's. The claim, nor the intention of the report is the complete development of a new cyber actor typology. Instead, the report describes the first cycle that would lead to the design of a new cyber actor typology. The report and the method outlined in it are explicitly designed to facilitate use by threat intelligence analysts and other cyber security practitioners to continuously improve and update the Dutch cyber actor typology. The research project divides the development of the threat actor typology in three subsequent steps:

Cycle one: deductive approach

In the first cycle, a structured model of (potential) cyber threat actors that (could) threaten Dutch data systems is created. As a starting point, a concise literature research was conducted to identify the dimensions that are used in (cyber) threat actor typologies. Google Scholar and (academic) databases Elsevier Scopus and IEEE Xplore were searched in search of literature displaying useful methods to generate a threat actor typology or a completed threat actor typology. Using a limited number of search terms yielded a selection of publications which could be further reduced based on closer review and resulted in a data base of some 70 publications that seemed to hold potentially relevant information for the development of an initial threat actor typology.

The main finding of the literature research is that no generic concise threat actor typology can be identified and underlying information regarding the methods used and the construction of the typologies are often unclear. However, despite these findings, a certain common basis for building a cyber attacker typology emerges. Five dimensions which form the core of the typology are identified: 'target', 'expertise', 'resources', 'organization', and 'motivation'. However, they are often inadequately conceptualized and operationalized to identify (threat actors).

A second step in the deductive phase entails the conceptualization and operationalization of the dimensions. After having operationalized the five dimensions of the typology design, it could be argued that the theoretical challenge of the design of the typology is complete. With the identification of the key threat actor dimensions and the subsequent operationalization of the dimensions a finite range of possible cyber actor types can be identified. The sheer amount of potential threat actor types, however, would make the typology simply unusable.

To support practitioners, an intermediate product is developed that allows analysts and practitioners to create a manageable set of threat actor types, and a tool to support the actor classification process and add rigor to it, which contributes to the method of the development of a new cyber threat actor typology and its cyclic nature. The tool – a so-called cyber threat actor typology framework – is designed as a concise set of questions that supports analysts to quickly classify incidents or an attack (scenario) and subsequently identify threat actor types behind security incidents. Like the typology, we do not claim to provide the definitive cyber threat actor typology framework. In the interview round with stakeholders, continuous improvements were made in the treat actor typology, its dimensions and the design of classes in the threat actor typology framework. Apart from cyber security experts and

stakeholders, the threat actor typology framework was validated via a workshop with 5 NCSC and NCTV analysts and advisors on February 23rd, 2017. Based upon the feedback from the interviews and the workshop, a final redrafting of the threat actor typology framework was undertaken. The framework is provided as a separate deliverable in this project and forms an integral part of the method that is developed.

Cycle two: inductive approach

The inductive approach forms a second additional, parallel step in the development of a method to develop a threat actor typology. It involves the systematic process of extracting threat actor information from available empirical data sources: specific incidents, large-scale measurement data, victim surveys, interviews with experts, etc., to analyse developments and trends. Behaviour of threat actors and characteristics of threat actor types are identified by analysing data. Empirical data is thus used to feed the threat actor typology and potentially yields additional information about threat actor types, enabling reflection and improving upon the inductively deduced threat actor typology. In particular, the main source of information to gather intelligence of cyber threat actors are: Honeypot data, Sinkhole data, Darknet/IDS data, Spam trap data and Cyber criminal markets. The research analyzes several case studies to provide examples of how these datasets can be leveraged to feed the cyber actor typology.

Result: Coming full circle with a new threat actor typology

In the two cycles provide the building blocks for the development of the new threat actor typology, which forms the third step. From the deductive cycle, the threat agent typology framework was used. This threat actor typology framework was fed with the information from the inductive cycle and the information of about roughly 50 different trends, vulnerabilities, attacks and attack scenarios provided in the CSAN 2016.

Via an intermediate categorization step which sought to cluster the various attack types and motives, the available information from the inductive cycle and the CSAN 2016 yielded 11 cyber threat actor types: extortionists, information brokers, crime facilitators, digital robbers, scammers and fraudsters, crackers, insiders, terrorists, hacktivists, state actors and state-sponsored networks. For each threat actor type, and each (conceivable) attack scenario, the framework typology can be used to classify the threat and link it to a threat actor type. This research has utilized the (limited) available information provided in the CSAN 2016 to plot the threat actors. When specific information on an attack is missing, a plausible or conceivable attack scenario will be provided. Based on these short descriptions the researchers will ‘plot’ the characteristics of the identified threat actor types to create a first threat actor typology. The plot is provided in Table 2 on the page 8.

As a consequence of the structured application of the proposed method, the new threat actor typology differs significantly from the typology provided in the CSAN 2015 and 2016. A summary in which the major differences are highlighted is provided in Table 1.

Most if not all of the threat actor types from the CSAN typology have found their place in a new threat actor type. In addition a few new threat actor types are added. The various threat actor types are clustered according to their motivation.

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'	

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

First of all the heterogeneous threat actor type professional criminals who share the economic motivation for attacks has been split into different threat actor types based on attack type or specialization. Implicitly this was also done in the CSAN but this distinction has been made much more explicit in the new threat actor typology and allows for a simpler classification and a more focused characterization of the behavior of threat actor types.

Second, the threat actor type state actors in the CSAN 2016 typology conducts attacks because of geo-political motives. In the new threat actor typology the single threat actor type is split into two differ threat actor types. Both of these new threat actor types are still geo-politically motivated. One displays (traditional) types of attacks (espionage) which can be attributed to state actors. The second threat actor type conducts different types of attacks. Instead of relying on stealth, attacks are conducted more overtly, but above all are organized markedly differently. The organizational constellation takes network characteristics and consists of more actors.

The actor groups terrorists, cyber vandals and script kiddies and hacktivists which were distinguished in CSAN have been merged and/or renamed in the new threat actor typology. What primarily characterizes this rather heterogeneous group of threat actor types are their motives which are non-economic.

The actor type cyber vandals and script kiddies have been renamed into crackers. The overriding goal of crackers is to conduct attacks for personal motivation (e.g. fun or reputation). Crackers with different levels of expertise can be identified (e.g. wannabe's who display low levels of expertise and resources, and medium experienced crackers with medium levels of expertise and/or resources). Both subgroups within the threat actor type seem unable or incapable to employ medium to high levels of resources in their attacks.

Terrorists and hacktivists reappear as threat actor types but they are more rigorously differentiated from each other. They share an ideological motivation and do not markedly differ when their behavior is analyzed using the proposed new threat actor typology framework. They differ in that they (often) focus their attacks on different categories of targets. Furthermore the impact sought with the attacks differs markedly between both groups. Compared to hacktivists terrorists seek maximum societal impact which translates into attacks which are designed to inflict maximum destruction and/or casualties. However, this characteristic does not feature as a dimension in our typology. However, the marked difference between the two groups is important to distinguish. For this reason and the latent,

but persistent threat, this threat actor type is 'reserved' for the type of destructive attacks that also characterizes this group in the physical domain. The threat actor type is ‘predicted’ even though no data supports the actual existence of such threat actors.

The threat actor insider comprises only the sub-dimension ‘disruption of IT’ in the CSAN threat actor class ‘internal actors’. Insiders are (former) employees who conduct attacks for personal motivation. The attacks in which internal actors are involved for economic gain are incorporated in the characterization of the organizational constellation of the kill chain, often indicating also higher resources in terms of preparation and higher levels of expertise. However, individual attacks of insiders remain which might have different sources of motivation.

Finally, three threat actor types which feature in the current CSAN typology are missing: cyber researchers, private organizations and ‘no actor’.

The absence of these actors from the threat actor typology can be explained. First of all, private organizations as threat actors are included, or absorbed if you will, in the various cyber criminal threat actor types as a result of the inclusion of an organizational dimension in our threat actor typology.

Second, cyber researchers are in themselves not necessarily attackers even though they might have a financial motivation to engage in research to identify vulnerabilities. For example, cyber researchers and white hackers often do research to identify vulnerabilities for financial motivation. A company that investigates zero days and sells that information to a company who employs or makes the product is not a threat actor; the company does not take part in the attack. Bug bounties similarly do not qualify as attacks in our opinion since an invited attack seems paradoxical. So unless research (in)advertently causes a direct breach of the CIA of systems, cyber researchers are not attacking, but investigating vulnerabilities. In fact, this line of argumentation matches with the guidelines which were provided with the typology framework: unintentional attacks are not considered to yield relevant results and do not identify a threat actor type. However, often, exploits or vulnerabilities identified by cyber researchers are subsequently employed by other threat actors in attacks. But that does not necessarily make the cyber researcher a threat actor (or part of a threat actor).

However, the role of the hacker or researcher changes significantly when not only there is an economic motivation but when the researchers becomes an active part of a kill chain; i.e. when a hacker or researcher actively distributes (i.e. sells) the exploit to a client (e.g. a criminal or a state actor (law enforcement agency). This line of reasoning eliminates the distinction which is often made between grey and black market cyber researchers and hackers. An example that perfectly illustrates our distinction in terms of the role of the cyber researcher is the ‘Hacking Group’ case.

The third threat actor type ‘no actor’ can clearly be considered misplaced in a threat actor typology and is therefore removed. That does not mean that the authors do not consider security incidents which appear to have no threat actor to be irrelevant or unimportant as sources of vulnerabilities. However, they simply have no place in the threat actor typology. Incidents which result from natural causes or technological or socio-technological complexity are in need of analysis and evaluation by security practitioners but should not be part of this specific security analysis. Instead of the threat actor type 'no actor' the threat actor typology framework does identify the motivational class ‘unintentional’, pointing towards the possibility of inadvertent threats resulting in security breaches. However, according to the authors, the application of unintentional motives in the threat actor typology framework requires interpretation of incidents and scenarios in counterintuitive ways, which does not seem to

contribute much to the overall goal of the typology. Consequently, as a threat actor type unintentional actions are not translated into a specific threat actor type.

The research set out to update the cyber actor typology that has been used in the 2011-2016 CSANs. A new cyber threat actor typology design method is presented. However, as pointed out before, the threat actor typology that is developed in this report is not intended as the definitive version of a threat actor typology. It was based on a first complete development cycle but used only limited data to feed the threat actor typology framework. Validation of the threat actor typology would require more analysis and more data.

	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										■	■

Table 2: Threat actor typology based on CSAN 2016