

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

Towards a new cyber threat actor typology

A hybrid method for the NCSC cyber security assessment

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

Preface

This report could not have been made without the help of a large number of people. We cannot mention all of these people by name, but our thanks extends to all of them. First of all, the researchers would like to thank all the interviewees, who were promised anonymity, for their precious time and valuable feedback. They have contributed a lot to the report and our understanding of cyber actors and the methods which can be used to classify them. We, furthermore, would like to extend these thanks to the members of the supervisory committee. The committee consisted of Prof. Stijn Ruiter (chair), drs. Olivier Hendriks, drs. Noortje Henrichs, dr. Jan Kortekaas, Prof. Eric Verheul, and drs. Wytske van der Wagen. We appreciated their critical and highly constructive feedback during the entire process.

Needless to say, the usual disclaimer applies: The contributions from respondents or members of the supervisory committee do not mean that the respondents, members of the supervisory committee or these institutions automatically agree with the complete content of the report. Also, we would like to emphasize that the report does not necessarily reflect the opinion of or the Minister or the Ministry of Security and Justice.

*Mark de Bruijne
Delft, July 2017*

Contents

Executive summary 5

Leeswijzer 5

1 Introduction 6

1.1 Research aim, research questions and delineation 6

1.2 Reader's guide 7

2 Designing a method for a cyber threat actor typology 9

2.1 What is a cyber actor typology? 9

2.2 What should the cyber actor typology do? 10

2.3 The CSAN typology and its shortcomings 11

2.4 Criteria for a good threat actor typology 14

2.5 A method to develop a typology – building the framework 15

3 The deductive approach – threat actor typology framework 19

3.1 Literature review: in search of threat actor dimensions 19

3.2 Operationalizing the dimensions: developing the framework 25

3.3 Feedback on the framework from experts and stakeholders 30

3.4 Observations and feedback from NCSC/NCTV workshop 35

3.5 Final threat actor typology framework 38

4 The inductive approach – data analysis 44

4.1 Spam trap data 44

4.2 Honeypot data 48

4.3 Darknet data 51

4.4 Cyber criminal markets 52

5 A tentative new threat actor typology 54

5.1 Key features of the method to develop a threat actor typology 54

5.2 Application: combining the deductive and inductive cycles 55

5.3	A first version of a new threat actor typology	57
5.4	CSAN 2016 typology and new threat actor typology compared	62
5.5	Reflection and some final thoughts	64
Bibliography		67

Executive summary

For some years, the NCSC/NCTV has been using a cyber threat actor typology in its annual Cyber Security Assessment Netherlands. It has evolved over time and captures a set of actors with different motives, intentions and capabilities. 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 cyber security 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 actor typology. Section 3.5 contains a concise description of the framework, to be used as a standalone document. As part of the method description, we also develop a tentative new typology. This can be found in Section 5.3.

Leeswijzer

Het NCSC/NCTV gebruikt deze in haar jaarlijkse cyber security beelden een zogenaamde cyber actor typologie. De typologie die momenteel gebruikt wordt bestaat al weer enkele jaren en is gedurende deze periode geëvolueerd. Op een vrij intuïtieve wijze vangt de huidige typologie een aantal actorgroepen met uiteenlopende motieven, intenties en capaciteiten. 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 en systematische methodiek die het NCSC/NCTV in staat stelt om de typologie voortaan zelf regelmatig up-to-date te houden. Paragraaf 3.5 bevat een compacte beschrijving van de methodiek die bedoeld is om als losstaand document gebruikt te worden door analisten. Als onderdeel van de methode wordt een eerste versie van een nieuwe typologie ontwikkeld. Die is opgenomen in paragraaf 5.3.

1 Introduction

In the Netherlands, the responsibility for threat analysis in the digital domain is allocated to the National Coordinator for Security and Counterterrorism (NCTV). The National Cyber Security Centre (NCSC) is part of the Cyber Security Department of the NCTV and publishes an annual Cyber Security Assessment Netherlands (CSAN) (cf. NCSC, 2015; 2016). This assessment has been compiled since 2011.

The CSAN offers “insight into the developments, interests, threats and resilience in the field of cyber security over the past year. It is aimed at policymakers in government and the critical infrastructure sectors to help enhance the digital resilience of the Netherlands or to help improve current cyber security programmes” (NCSC, 2015:15).

Both public and private organizations contribute to this annual cyber security assessment, as well as make use of it. The CSAN features a cyber actor typology to provide insight in the threats and threat actors. In the 2016 Cyber Security Assessment Netherlands (CSAN) the actors in this typology are defined as individuals or groups “who adversely affect the reliability and security of information and information systems” (NCSC, 2016:25).

The current cyber actor typology has been existence for some years. It evolved over time and it intuitively captures a set of actors with different motives, intentions and capabilities. In view of its age, NCSC/NCTV inquired whether the current cyber actor typology is still valid today and supported or rejected by recent insights from science and cyber security practice and in need of improvement. This research project, which was commissioned by the WODC (Research and Documentation Centre) of the Ministry of Security and Justice aims to address this knowledge gap.

1.1 Research aim, research questions and delineation

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, designed to be more transparent than the typologies used in CSAN 2016, and features a structured way to classify threat actors.¹ The method is designed in such a way that it can be repeated over time. 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. We will discuss the implications of this delineation in subsequent chapters of the report.

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 (NCSC, 2016). 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

¹ See <https://www.ncsc.nl/english/current-topics/Cyber+Security+Assessment+Netherlands>, last visited May 15, 2017.

method to develop the cyber actor typology on an ongoing basis. In view of their national responsibility for threat analysis in the digital domain, this research particularly supports practitioners in the National Coordinator for Security and Counterterrorism (NCTV) and the National Cyber Security Centre (NCSC) in performing this crucial function. However, the method and typology presented are explicitly designed to be more broadly applicable as well.

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?

In response to this research project proposes the development of a new method to incrementally improve the current cyber actor typology. As a practical limitation, the cyber actor typology should be restricted to the description of actors who either operate from The Netherlands or (intend to) focus their attacks on The Netherlands.

The method features a structured analysis of (potential) cyber threat actors as well as a structured approach on how to use more (diverse) data sources to update the cyber actor typology in the (near) future. 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 experts to continuously improve and update the Dutch cyber actor typology.

A third practical limitation is that the research pays particular attention towards the possibility for potential collaboration between different cyber threat actors, which has been reported as an increasingly complexifying trend in cybersecurity (cf. CSAN, 2016). This focus is highlighted in the research questions (in particular research question 3), which means that this element features prominently in the analysis of cyber actors and the search for key characteristics to analyze them. The overarching goal is to develop a design method that supports ongoing, incremental development and improvement of the cyber actor typology. We will reflect on this design choice and the implications for the long-term validity of (design of) the threat actor typology in the report.

1.2 Reader's guide

In the first chapter, the main method to develop a cyber actor typology is designed. The report unpacks and articulates the various terms and terminologies that surround the typology and identifies the intended use of the typology. The report subsequently explores the underlying complexity and challenges of the design of such a typology. Next, we outline the limitations of the CSAN typologies. Criteria are drawn up to identify quality indicators for a cyber threat actor typology. Finally the new method is proposed to fulfil these criteria and to allow for the creation of a valid and useable cyber threat actor typology. The method 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.

In Chapter 3, the first part of the method is developed: the deductive cycle. To bootstrap the design of a threat actor typology, a literature review identifies common dimensions from existing typologies of threat actors. To enrich the literature research and ensure the development of a threat actor typology that is fit-for-purpose, recent insights and feedback on the theoretically deduced dimensions were collected via interviews with cyber security experts and stakeholders. The result is a ‘deductively’ developed set of key dimensions that forms the starting point of the new method to develop the threat actor typology.

With the key dimensions in hand, the report proceeds to combine them into a framework and operationalize them for use by threat intelligence analysts and other experts. The framework is explicitly designed to support practitioners in the threat classification process. Section 2.2 describes the design and subsequent updates which culminated in a final version of the threat actor typology framework.

Chapter 4 turns towards the second part of the proposed method to develop a cyber actor typology: the inductive cycle. This cycle draws on empirical data about incidents and attacks, available information on online behavior, which is analyzed and fed in the threat actor typology. Using several datasets which the researchers had at their disposal, it is illustrated how incident and attack data can be used to gain more insight into certain dimensions of the actor typology – and is less informative about other dimensions. The chapter reflects on the added value of large-scale measurement data and how it contributes to current knowledge and understanding of attackers and their routines.

Chapter 5 presents the culmination of the previous chapters: a tentative new threat actor typology resulting from a completed deductive and inductive cycle. Since the proposed method for the development of a threat actor typology in this research project has only completed a single development cycle, and is thus limited in terms of the underlying data, the chapter ends with a condensed set of development guidelines and discussion points to support the subsequent threat actor typology design cycle by NCSC/NCTV.

2 Designing a method for a cyber threat 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’. Next the report explicates on the intended use of this cyber actor typology in the annual Cyber Security Assessment Netherlands (CSAN). This is necessary to align what the final products—the method and the resulting cyber actor typology—actually need to ‘do’.

2.1 What is a cyber actor typology?

The on-line Merriam-Webster dictionary defines a typology as: “a system used for putting things into groups according to how they are similar: the study of how things can be divided into different types.” In other words, a typology is a specific form of classification. Bailey (1994:4) claims that “two characteristics distinguish typologies from generic classifications. A typology is generally multidimensional and conceptual.” A typology is appealing because it promises to yield a concise yet parsimonious framework to describe and classify observed patterns. Bennett & Elman (2006:466, Table 1) identify three different subtypes with distinctly different goals (cf. Clinard, Quinney & Wildeman, 1999:13):

1. Descriptive typologies which answer the question: ‘what constitutes this type’?
2. Classificatory typologies which answer the question: ‘what is this a case of’?
3. Explanatory typologies which allow researchers to extend—if my theory is correct: ‘what do I expect to see? Do I see it’?

The definition and identification of different goals, that can be served by typologies also forces us to briefly consider and distinguish typologies from other terms can be encountered in cyber actor research literature, such as the terms ‘taxonomy’ and ‘profiles’. A ‘taxonomy’ is defined by Merriam-Webster as: “the process or system of describing the way in which different living things are related by putting them in groups” and a ‘profile’ as: “a brief written description that provides information about someone or something”. For the intents and purposes of this report, both cyber actor taxonomies as well as profiles of methods from cyber attacks or cyber attackers provide valuable input on important characteristics of cyber attacks or cyber actors which seem relevant for the creation of a cyber actor typology. Yet, they are not the same. The report returns to this issue later. Sufficient for now is that there exists a clear distinction between taxonomies and typologies and that typologies are generally used in the social sciences (cf. Seebruck, 2015:37). In a typology, the dimensions are made up of concepts which should be considered as “as ideal types rather than empirical cases, meaning typologies are not necessarily exhaustive” (Ibid.). Typologies can thus be defined as “conceptually derived interrelated sets of ideal types” (Doty & Glick, 1994:232). Taxonomies on the other hand “categorize dimensions based on empirical observation and measurable traits” (Seebruck, 2015:37).

After having shortly identified what a typology is, and having identified its various subsets and distinguished it from other related terms, the research continues and explicates and aligns its terminology with intended use of NCSC/NCTV and the employed method to build such a cyber actor typology.

2.2 What should the cyber actor typology do?

A logical second question of the report would be to establish the intended goal that the cyber actor typology would serve. In the introduction the project's research goal was identified based on the tender request: to assess and if needed update or improve the NCSC/NCTV typology to help security professionals in their efforts to identify and assess threats from actors who "adversely affect the reliability and security of information and information systems" in the Netherlands (NCSC, 2016:25).

Obviously, the cyber actor typology and its underlying method need to produce a reliable output, i.e., when different analysts use it, they should identify a more or less consistent set of threat actors. Typology and underlying method therefore need to adhere to scientific design criteria such as consistency, dependability and replicability. That being said, analysts will face certain trade-offs during the use of the method, such as more precisely distinguishing different threat actors versus ending up with a manageable number of types in the typology. Different analysts might make these trade-offs differently based on how the resulting typology is to be used.

Given the central role that the cyber actor typology plays in threat assessment in The Netherlands and the highly dynamic environment in which it is embedded, NCSC/NCTV staff members will have to work with the typology on a day-to-day basis. This requires not only a reliable, but also a concise typology.


The typology needs to be unambiguous, i.e. (intuitively) clear to its (wide range of) intended users and must be able to capture the key characteristics of all (potential) cyber actors in a small set of dimensions which in turn would systematically lead one to identify a threat actor type based on the available data or assumptions on each of the dimensions. To be more precise, the cyber actor typology only needs to categorize threat actors who are defined as actors who (intend to) "adversely affect the reliability and security of information and information systems" in the Netherlands (NCSC, 2016:25).

Various online activities such as child pornography distribution, copyright infringement, and cyberbullying do not infringe on those security requirements and are therefore not included in the typology as a threat actor even though obviously they are conducting illegal activities. The cyber actor typology is therefore not the same as a cyber criminal typology. To ensure this crucial distinction is more intuitively kept, the term 'threat actor typology' will be used from here on in the report.

To conclude: the threat actor typology for NCSC/NCTV creates 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).

Table 1 Threat matrix

Source of the threat	Targets		
	Governments	Private organisations	Citizens
Professional criminals	Theft and publication or selling of information	Theft and publication or selling of information	Theft and publication or selling of information
	Manipulation of information	Manipulation of information	Manipulation of information
	Disruption of IT	Disruption of IT	Disruption of IT
	IT takeover	IT takeover	IT takeover
State actors	Digital espionage	Digital espionage	Digital espionage
	Offensive cyber capabilities	Offensive cyber capabilities	
Terrorists	Disruption/takeover of IT	Disruption/takeover of IT	
Cyber vandals and script kiddies	Theft of information	Theft of information	Theft of information
	Disruption of IT	Disruption of IT	
Hacktivists	Theft and publication of obtained information	Theft and publication of obtained information	
	Defacement	Defacement	
	Disruption of IT	Disruption of IT	
	IT takeover	IT takeover	
Internal actors	Theft and publication or selling of information	Theft and publication or selling of information	
	Disruption of IT	Disruption of IT	
Cyber researchers	Receiving and publishing information	Receiving and publishing information	
Private organisations		Information theft (industrial espionage)	Commercial use/abuse or 'resale' of information
No actor	IT failure	IT failure	IT failure



Change with respect to CSAN 2015.

<p>No new trends or phenomena are recognised that pose a threat.</p> <p>OR</p> <p>(sufficient) measures are available to remove the threat.</p> <p>OR</p> <p>No appreciable manifestations of the threat occurred during the reporting period.</p>	<p>New trends and phenomena are observed that pose a threat.</p> <p>OR</p> <p>(limited) measures are available to remove the threat.</p> <p>OR</p> <p>Incidents have occurred outside the Netherlands and there have been several minor incidents in the Netherlands.</p>	<p>There are clear developments which make the threat expedient.</p> <p>OR</p> <p>Measures have a limited effect, so the threat remains substantial.</p> <p>OR</p> <p>Incidents have occurred in the Netherlands.</p>
--	---	---

Table 1: 2016 CSAN threat actor typology. Source: NCSC, 2016:12. Table 1: Threat matrix

2.3 The CSAN typology and its shortcomings

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) in more detail (cf. NCSC, 2016).

The origins of the typology used in the 2016 version of the Cyber Security Assessment Netherlands (CSAN) can be traced back to the CSAN 2011 (Govcert.nl, 2011). The original typology identified 6 cyber actor types² in 2011, which was extended into 9 cyber actor types in the following 2012 issue (NCSC, 2012). From 2012 until 2016 the cyber actor typology remained basically unaltered. The 2016 cyber actor types can be seen in the 2016 CSAN threat actor typology here reproduced as Table 1.

After having identified and articulated the intended use of the desired cyber threat actor typology, shortly discussing CSAN's cyber actor typology, three major shortcomings and weaknesses of the CSAN cyber actor typologies can be identified:

2.3.1 Lack of consistent dimensions for distinguishing actors

The typology in the CSAN 2016 identifies 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 (cf. CSAN, 2016). The lack of a transparent, explicit and systematic methodology can be traced to the original typology which was “primarily distinguished based on intention” (Govcert.nl, 2011: 17) [translated from Dutch], but also acknowledges that other threat actor characteristics (resources, volume which is used as an indicator for the amount of attacks and visibility) play a role in the classification process. 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.

For example, the difference between the actor groups ‘cyber vandals’ and ‘hacktivists’ in the 2016 CSAN seems to be based not on intention, but on capability: low versus high. Yet this dimension—capability—is not applied systematically in the typology.

Furthermore, ‘professional criminals’ and ‘terrorists’ are not clearly distinguished by capability, but rather by motive: profit versus fear. The dimension of motive is also not systematically articulated. Certain motives seem to be missing such as individuals attacking other individuals for personal revenge.

To make matters even more muddled, the current typology also includes ‘private organizations’ as a threat actor type, which is a vague category that overlaps with ‘hacktivists’, ‘cyber researchers’ and ‘internal actors’.

As a final illustration of the need for a more systematic underlying framework, we point to the paradoxical ‘no actor’ category in the typology. This category is out of place in a threat actor typology, which is designed to classify actors, who (intend to) “adversely affect the reliability and security of information and information systems” (NCSC, 2016:25).

2.3.2 No systematic methodology to revise actors or define new actors

Any typology should be adjusted to dynamics. After all, typologies are “historical, time-bound mental constructions” (Clinard et al., 1994:12) and therefore need to be reviewed periodically. Due to the lack of a systematic set of dimensions on which the typology is based, it is also hard to put in place a systematic procedure to review and update the identified threat actor types. This has led some threat actor types to mushroom into very heterogeneous aggregates of actors. The 2016 CSAN typology in short shows that it is

² These were: professional criminals, state actors, terrorists, script kiddies, hacktivists, and private organisations.

primarily fed by data about (recent) events and trends rather than any threat analysis. The most notable example is the threat actor type 'professional criminals', which covers a much wider range of actors than the categories of 'script kiddies' or 'cyber researchers', for example and does not seem to be fed on similar types of information which would allow one to infer certain threat actors.

An even more problematic consequence is that the current typology misses threat actors that are emerging, but which get lumped into existing categories. Consequently, over time there is a high chance that the typology will become less and less informative. This can already be seen with the current typology. For example, an important actor type that emerged over the last few years are private actors that seem to be recruited for state-sponsored attacks. For example, attacks identified by western security firms as part of Operation Pawn Storm, all seem related to a group of hackers also known as Pawn Storm, Fancy Bear or APT28, (cf. Kharouni et al., 2014; Hacquebord, 2017; Perlroth, 2017). The group allegedly attacked a wide variety of economic and political targets in a rather brazen manner. Claims are made that the group works for the Russian state or the Russian state intelligence services (cf. Perlroth, 2017, Fox-Brewster, 2017), but the state keeps the actual attacks at a certain distance (cf. Higgins, 2017).

Since the attackers are not associated directly with the state, they do not seem to care very much about being discovered. In practice, this means they can work in a more overt, standardized and efficient way than state cyber intelligence forces. Where would they fit in the current threat actor typology? They do not fit well in the category of 'states', because the attackers can be less circumspect and go after more targets against lower cost. Nor do they easily fit in the category 'professional criminals', because the crime itself has no monetization strategy for the acquired information resources on the criminal market. The money is earned because there is a client for the attack.

Pawn Storm

According to cyber security company Trend Micro, the group of threat actors known under the heading Pawn Storm are capable of "long-term operations", and conduct different types of "attacks that can last for years". In their 160 campaigns, the group is known to employ "simple but oftentimes well-prepared credential phishing" (Hacquebord, 2017:9) as well as spear phishing methods (Kharouni et al. 2014). Targets include US defense contractor personnel, Russian dissidents, international media, the Organization for Security and Co-operation (OECD), the US Democratic National Committee, and the presidential campaign of Emmanuel Macron. The group employs various tactics, displaying technical as well as social engineering expertise in the employment of zero-days. However, at the same time the group distinguishes itself because of its lax operation security, meaning that it does not seem to care if their attempts are identified at some point. In fact at certain points the group "uses mainstream media to publicize their attacks and influence public opinion" (Hacquebord, 2017:5).

Another example is the emergence of new actors that enter the cyber crime market because of the commoditization of certain types of cyber crime. One such example comes from a recent analysis of DDoS amplification honeypot data (Noroozian et al., 2016). The study concluded that the so-called booter services are rarely used for large attacks on valuable targets, like banks or governments. Instead, over 60% of the targets are regular end users. Thus, it could be inferred that most of the attackers are also regular end users and that many attacks take place around online gaming. These attacking end users could be lumped in with 'cyber vandals', but this again muddles the typology by conflating different motives. The aim of these attackers is not to vandalize public resources, but rather to tease or harass their own

friends and fellow gamers. In other words: the commoditization of cyber crime leads to a democratization of attackers and new groups enter the attack landscape around online gaming.

2.3.3 Under-utilization of large-scale measurement data

As the previous examples already illustrate, the current typology lacks a mechanism to take advantage of ongoing measurement data generated all over the landscape by honeypots, sandboxes, darknets, netflow monitors, passive DNS monitors, intrusion detection systems, et cetera. While the CSAN's do provide information on measured trends, it is unclear how they lead to changes in the threat actor typology. The trends that are described in the CSAN seem to be implicitly attributed to the already identified threat actor types, reinforcing the existing typology. This 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, which can distinguish new actors that look similar on some dimensions, but are different on relevant other dimensions and thus need to be distinguished. See the example of private attackers providing intelligence services to state with criminal strategies and the example of regular users going after friends via commoditized crime services.

Any new method that would result in the development of a cyber threat actor typology would have to address and preferably solve these shortcomings.

2.4 Criteria for a good threat actor typology

After having established the goal of the project and identified shortcomings in previous threat actor typologies for which solutions are sought, this report turns towards the identification of a set of 'quality indicators' that would enable one to distinguish an improvement in the proposed method from the previously used cyber actor typology. Literature provides some criteria to identify a good (threat actor) typology (cf. Lindqvist & Jonsson, 1997:155; Gundel, 2005:107; Bailey, 1994:3):

1. Classes formed via the typology must be exhaustive (i.e. all potential threat actors should be classified).
2. Classes formed must be mutually exclusive (i.e. all potential threat actors fit in just one of the classes).
3. The threat actor typology must be relevant (i.e. the intended goal of quick, consistent replication based on available information allows for meaningful classification of events).
4. The threat actor typology must be pragmatic (i.e. the number of subsets should be manageable and heterogeneity between the subsets should be ample to enable relatively quick classification). By necessity the threat actor typology must therefore be composed of types at a fairly high abstraction level.

Furthermore, based upon the intended goals and identified shortcomings, additional criteria can be formulated:

5. The threat actor typology must allow for efficient classification of threat actors (section 2.2)

6. The threat actor typology must be based on a clear set of dimensions and the process of classification must be transparent (section 2.3.1).
7. The threat actor typology must be dynamic. A method should be provided that allows for the possibility to continuously update the threat actor typology based on new data and insights (section 2.3.2 and 2.3.3).
8. Classes in the typology can be changed as a result of criterion 7. New classes can be formed in the typology (section 2.3.2 and 2.3.3).

It should however, be noted that these quality criteria for threat actor typology designs, in themselves are potentially conflicting. For example, a method that would be considered to satisfy criterion 1 might yield a more complete threat actor typology, but at the risk of violating criterion 4, the ability to enable quick classification and yield a manageable and meaningful number of threat actor types. In short the new threat actor typology design method would have to strike a motivated balance between these criteria. This balance and the arguments behind the choice of the threat actor typology design will be provided in the remainder of this report.

2.5 A method to develop a typology – building the framework

As a first step to develop a threat actor typology a systematic method to clarify, revise and enrich the CSAN threat actor typology needs to be explained step by step.

As a starting point for the design of a systematic method, a ‘combined’, hybrid conceptual/empirical level classification procedure can be identified (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.

The deductive approach defines general properties or dimensions of threat actor types. The deductive phase starts by analyzing the observed distinguishing characteristics of the threat actors: motives, capabilities, degree of organization, et cetera. Combining these dimensions results in a matrix of potential threat actor types who may or may not be observable in the current threat actor landscape. To use an analogy: the dimensions would serve to identify a set of threat actor types, like the periodic table does identify elementary particles in chemistry. Based on a number of key characteristics elements can be ranked, grouped and identified. Threat actors identified in practice would function like elementary particles to the whole table of elements. Like the periodic table of elements, the conceptual threat actor typology could take on a similar role as the table in the early 1900s when some of the elements (i.e. certain threat actor types) were not yet identified in practice. However, all elements eventually were identified and observed decades later. Some even because their existence was already inferred. Unfortunately, unlike the table of elements, a generic theory which would explain and predict cyber actor classes is (still) absent and therefore the analogy does not hold. The typology in this report therefore ‘merely’ enables users to systematically classify the cyber actor types.

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 analyze developments and trends. Behavior of threat actors and characteristics of threat actor types are identified by analyzing 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. Furthermore, the inductive approach is necessary to accommodate for the fact that cyberspace keeps on changing and cyber actors develop and employ new attack vectors every day. Their behavior is dynamic and may change over time with the acquisition of new skills (Jahankhani & Al-Nemrat, 2012). Empirical data helps to capture the dynamics. The other issue is that the data used in cyber security assessments are based on generalizations, and the sampling leaves out a dataset of cyber actors who avoid detection over a period of time, thereby introducing inaccuracies in the results (Noroozian et al., 2015). Relying on inductive methods only is unsuitable for a method that intends to produce a dynamic threat actor typology.

On the other hand, relying only on deductive profiling will leave investigators oblivious to current trends such as popular attack methods, likely targets and victims (Tennakoon, 2011). Therefore, a hybrid methodology is the logical remaining option to ensure the continuous development of threat actor profiling as part of a loop (Warikoo, 2014). The method thus assumes a cyclic character and results in a method that systematically creates a multi-dimensional set of characteristics of threat actors deductively and enriches this set with empirical information that was obtained by inductively analyzing cyber security datasets and reports.

The hybrid approach leverages a broader set of sources and methods to proactively collect and passively detect indicators and characteristics of threat actors, thus benefitting from the structured and continuous analysis of all potential data.

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 (cf. NCSC, 2015; 2016). The complete method can be visualized as a sequence of at least two loops, which feed back into the CSAN threat actor typology. The first loop deduces from existing literature key threat actor characteristics (i.e. motives, capabilities, degree of organization, etc.). When these characteristics are cross tabulated, a systematic and finite typology of existing and (yet) non-existing types of threat actors can be composed.

The second loop consists of an inductive approach which utilizes the available empirical data. Various methods such as data mining techniques can be employed to systematically identify and observe behavior of threat actors. A complete first iteration starting with the typology described in the CSAN 2016, followed by a loop in which a deductive approach is applied and then a loop in which information is inductively analyzed.

This method can be divided in three subsequent steps:

2.5.1 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 identifies the dimensions that are used in (cyber) threat actor typologies. To identify and construct a new threat actor typology, a somewhat broadened scope was chosen for the initial literature research. 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. The following keywords were used in various potential combinations as outlined in Table 2.

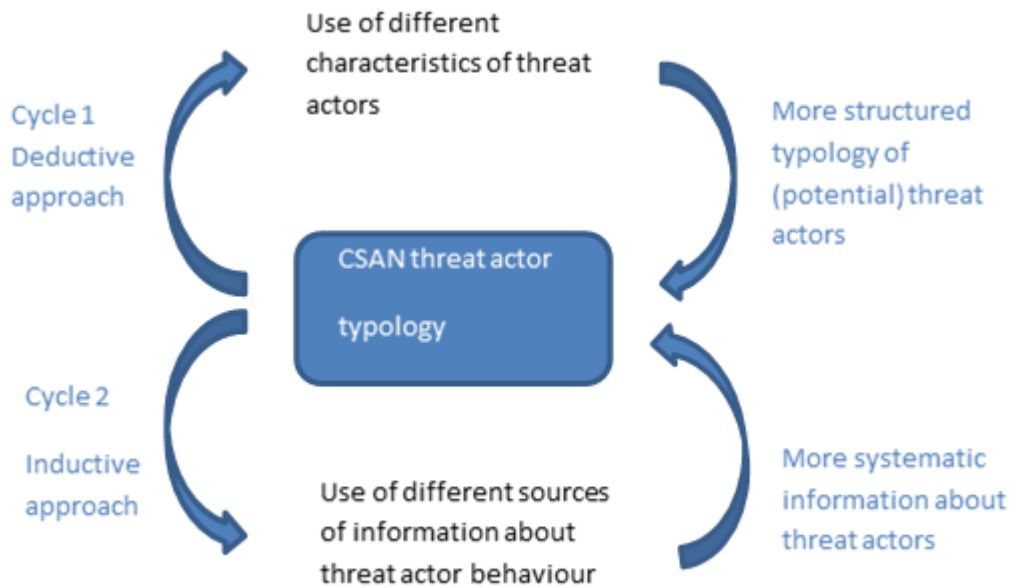


Figure 1: A hybrid method to develop a new threat actor typology

Using these 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 a threat actor typology. There exist several typologies and ways of classifying cyber actor and cyber criminals in particular based on their motives on which was built (e.g. Johnson, 2005; Jahankhani & Al-Nemrat, 2012; Rogers 2006). Also empirical interviews were conducted to identify relevant threat actor characteristics. In total 18, semi-structured in-depth interviews were held with security experts that are in a privileged position with regard to knowledge about threat actors. More details on the interviews can be read in section 3.3). The selection of respondents was based upon a desire to achieve overall representation of stakeholders ranging from hardware designers to software providers, IT service providers, banks, small and medium enterprises all the way to police agencies who either work with the threat actor typology or play an important part or are engaged in cyber security. Secondly, the classification scales are established. This allows NCSC/NCTV staff to perform the proper threat actor classification process themselves. To support the NCSC/NCTV staff in this task, a threat actor typology framework is developed as part of the method. In the interview round with stakeholders, the threat actor typology framework is validated and additional information obtained on relevant characteristics distinguishing threat actors from those which are less relevant (for the foreseeable future).

Cyber	Attacker	Taxonomy
	Actor	Profile
	Threat actor(s)	Typology
	Threat agent	
	Hacker	

Table 2: Keyword search strategy

2.5.2 Cycle two: inductive approach

In the second cycle – which actually was performed parallel during this research project – different databases that contain observations of cyber incidents are analyzed in small case studies. Four different types of empirical data are used in this report to show how this data could feed into the threat actor typology. Data was used from honeypot data, sinkhole data, darknet/IDS data, spam trap data, and data from cyber criminal markets. By analyzing the data and establishing correlations between certain events and/or types of behavior, certain characteristics common to the different threat actor characteristics resulting from the deductive phase can be inferred allowing classification and thus yielding valuable information about threat actor types in addition to the information obtained (through interviews) in the deductive phase (cf. Caltagirone, Pendergast & Betz, 2013):

1. Observations of digital meeting places. Research on meeting places where various cyber actors meet and communicate with each other, such as underground criminal markets aid in the identification of cyber actors. Anecdotal data on the behavior in these meeting places shed light on actors (Aston et al., 2009). Analyzing online forums in the marketplaces provides information on how specific cyber actors meet, how specific cyber criminal networks develop and what this means for the attack capabilities of these networks.
2. Analyzing cyber incident datasets. Cyber incidents can be used to understand not only the attack vector but also provide additional information on the behavior and capabilities of cyber actors. Datasets (such as SPAMHAUS blacklists, Anti-phishing working group phishers) and public datasets (such as Clean-MX phishers, Abuse.ch botnet) which were used in this project contain information about phishing sites, spam, botnet command, etc. Data mining and data warehouse techniques were used to analyze types of cyber incidents to obtain knowledge of cyberattacks and the threat actors involved in them.
3. Monitoring ongoing attacks. Apart from incident data, the information about threat actors can be improved by the addition of data obtained from observations about ongoing attacks (e.g. via honeypots and IDS logs). The information received via DSHIELD logs were used to provide additional insights on attacker behavior.
4. Analyzing data related to victims. Additional analysis of datasets could provide information about victims, which in turn could provide additional knowledge about characteristics of cyber actors (type of victims chosen (MO), geographic details about the cyber actor, information about defenses and associated skill levels of the cyber actor). Some cyber victim analysis has already been carried out by national law enforcement agencies. For example, London's police created a profile of the victims of cyber fraud over the twelve-month period of November 2014 to October 2015 (Police City of London, 2016).

2.5.3 The design cycle completed: developing a threat actor typology

The final step in the method consists of the creation of a threat actor typology making use of the data obtained in both cycles. This then completes the method and enables NCSC/NCTV to make use of the available information on threat actors. This cycle can be reiterated over time. For example if new attacks or new vulnerabilities emerge, the threat actor typology might be in need of review or reassessment. The consideration of how and when to engage in a second threat actor development cycle forms a crucial aspect of the proposed method.

3 The deductive approach – threat actor typology framework

Chapter three describes the first phase of the deductive part of the method to develop a typology. Literature review identified various bodies of literature and various typologies of threat actors and dimensions to bootstrap the development of an initial typology. As a subsequent step interview data and a workshop are used to operationalize the threat actor dimensions and develop a threat actor typology framework.

3.1 Literature review: in search of threat actor dimensions

3.1.1 Universal cyber threat actor typologies

In literature, a number of elaborate universal classifications of cyber attackers can be identified. One of the oldest is known as the 'Threat Agent library' (TAL) which can be seen in Figure 2. This library identifies 23 threat actor types which obtain a unique score along 8 different dimensions (Casey, 2007; Casey, Koeberl & Vishik, 2011). Each threat agent is separately and relatively extensively described, as can be seen in Figure 3.

A second, more recent generic classification scheme is developed by the European Union Agency for Network and Information Security (ENISA) and can be seen in Figure 4. This classification scheme, initially distinguishes seven threat actor types and is later expanded into 15 threat actor types which are identified via three dimensions: 'sector', 'capability' and 'motive' (Marinos, 2013:39; 2014; 2016).

Both generic threat actor typologies show the challenges involved in establishing a threat actor typology and the complexities of classifying threat actors. Although helpful and elaborate, their sheer size (i.e. the number of threat actor types and/or the number of dimensions on which they are based) raise question marks with regard to usability requirements. However, both typologies identify the dimension 'motivation' as the most relevant threat agent characteristic (cf. Pushpakumar, 2015; Van Hulst & Neve, 2008).

	Intent	NON-HOSTILE				HOSTILE																
		Employee Reckless	Employee Untrained	Info Partner	Anarchist	Civil Activist	Competitor	Corrupt Government Official	Data Miner	Employee Disgruntled	Government Cyberwarrior	Government Spy	Internal Spy	Irrational Individual	Legal Adversary	Mobster	Radical Activist	Sensationalist	Terrorist	Thief	Vandal	Vendor
Access (1)	Internal																					
	External																					
Outcome (1-2)	Acquisition/Theft																					
	Business Advantage																					
	Damage																					
	Embarrassment																					
Limits (max)	Tech Advantage																					
	Code of Conduct																					
	Legal																					
	Extra-legal, minor																					
Resources (max)	Extra-legal, major																					
	Individual																					
	Club																					
	Contest																					
Skills (max)	Team																					
	Organization																					
	Government																					
	None																					
Objective (1 or more)	Minimal																					
	Operational																					
	Adept																					
	Copy																					
Visibility (min)	Deny																					
	Destroy																					
	Damage																					
	Take																					
	All of the Above/ Don't Care																					
	Overt																					
	Covert																					
	Clandestine																					
	Multiple/Don't Care																					

Figure 1: TAL threat actors. Source: Casey, 2007:5. Table 1: Current Library of Threat Agents and Their Defining Attributes

	Insider	Common Tactics/Actions	Description
Civil Activist		Electronic or physical business disruption	Highly motivated but non-violent supporter of cause
Cyber Vandal		Network/computing disruption, web hijacking, malware	Derives thrills from intrusion of property, no strong agenda
Government Spy	■	Theft of IP or Business Data	State-sponsored spy , supporting idealistic goals
Government Cyberwarrior		Organizational, infrastructural, and physical business disruption	State-sponsored attacker with significant resources
Internal Spy	■	Theft of IP, PII, or business data	Professional data gatherer as a trusted insider
Irrational Individual		Personal violence resulting in physical business disruption	Someone with illogical purpose and irrational behaviour

Figure 2: Details on TAL's threat agents. Source: Casey (et al.), 2011:219. Figure 2: Sample subset of threat agents

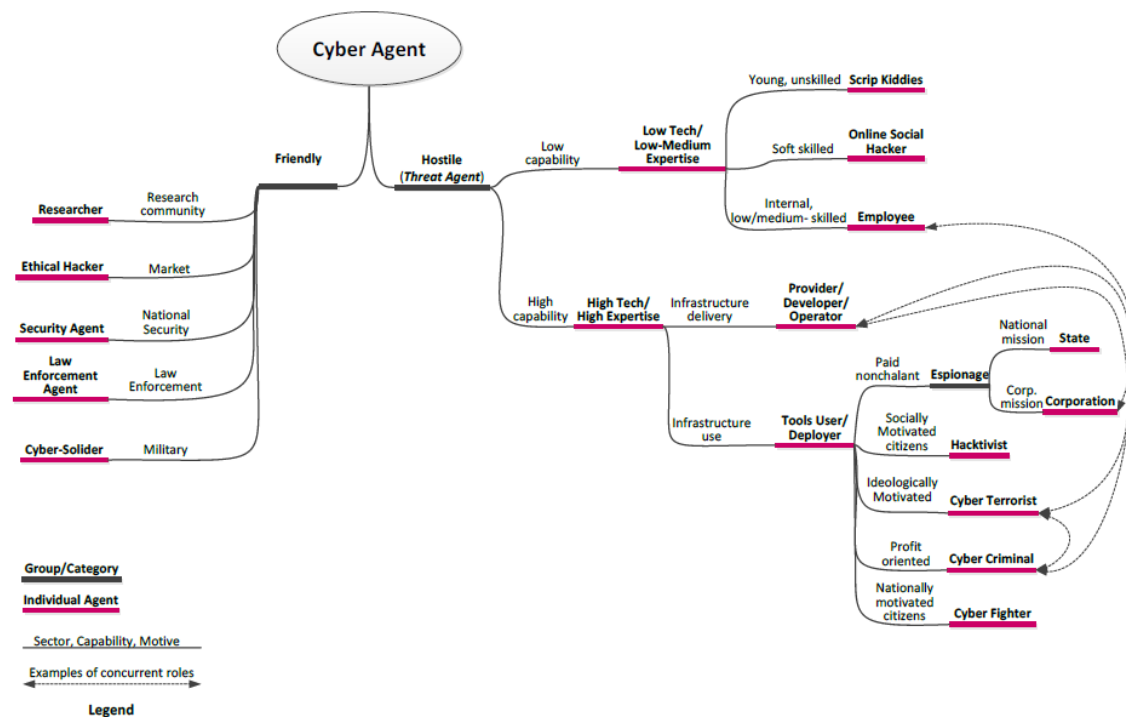


Figure 20: Overview of Agents in Cyber Space

Figure 3: ENISA's threat actor characteristics (sector, capability, motive). Source: Marinos, 2013:39. Figure 20: Overview of Agents in Cyber Space

3.1.2 (Inter)national cyber threat actor typologies

A second source of knowledge (to identify dimensions) for generic threat actor typologies can be identified in publications which identify, analyze and compare (inter)national cyber security policies and the typologies used (cf. Burton, 2015; Luijff et al., 2013; Robinson et al., 2013; Canbolat & Sezgin, 2016). Interestingly, some noticeable differences exist between various countries and their use of threat actor typologies. First of all, certain countries such as France and Finland had not (yet) published a public version of their cyber threat actor typology. Another distinction is the amount of threat actor types that can be observed in various national policies. The threat actor typologies in the Dutch CSAN (NCSC, 2015; 2016) are among the most detailed in use by nation states (cf. Robinson et al., 2013).

Other countries distinguish cyber threats from cyber actors. However, even here differences between the various threats and threat categories exist. For example, Burton (2015:299) identifies four cyber threats (cyber crime, cyber espionage, cyber terrorism, and cyber warfare), whereas for example, Canada identifies three broad types of threat (cyber espionage and military operations; terrorist use; and cyber criminal activity)(Sheldon, 2012:6). These broad threat types are further specified to produce more detailed threat actor typologies/taxonomies. To stick with the Canadian example: the broad threats are merged with empirically observed threat actor characteristics such as 'motivation', and 'attack types', which produces five cyber threat actors types: nation states, terrorists, criminal organizations, disgruntled insiders and hacktivists. Other studies (cf. Luijff et al., 2012) identify a similar range of threat actors: individuals, activists, criminals, terrorists, cyber spies, non-state and state.

This short review of national cyber actor typologies in cyber security policies illustrates that the typologies and methods on which nation states base their cyber security policies seem to differ substantively. Substantial differences in granularity of identified cyber threat actor types exist. However, all in all, nation states seem to identify “similar types of threat actor types” (organized crime, states and terrorist networks)(Robinson et al., 2013:40).

3.1.3 Typologies focusing on specific attack types

A third group of typologies in literature distinguishes threat actor types based on the attack type. For example, the U.S. Industrial Control Systems Cyber emergency Response Team identifies the following cyber threat actor types (for Industrial Control Systems): national governments, terrorists, industrial spies and organized crime groups, hacktivists and hackers. US Congress, however, identifies another set of threat actors in cyber crime ranging from “lone actors to expansive criminal networks or even nation states” (Finklea & Theohary, 2015:1).

Johnson (2005) and Jahankhani & Al-Nemrat (2012) argue that criminological dimensions based on classifications of past incidents could be used to identify cyber criminals. Key dimensions according to Johnson (2005:78) are ‘modus operandi’, “the actions taken by an offender to perpetrate the offense successfully” and ‘signature’, “a repetitive ritualistic behavior that the offender usually displays at every crime scene” (cf. Rogers, 2003:295, footnote 5). However, various sources mention a persisting lack of empirical knowledge of cyber attackers and their specific characteristics (cf. Van Hulst & Neve, 2008; Koops, 2010; Carrapico & Lavorgna, 2015).

Adversary Class	Skills	Maliciousness	Motivation	Method
script kiddies, newbies, novices	very low	low	boredom, thrill seeking	download and run already-written hacking scripts known as ‘toolkits’.
hacktivists, political activists	low	moderate	promotion of a political cause	engage in denial of service attacks or defacement of rival cause sites
cyber punks, crashers, thugs	low	moderate	prestige, personal gain, thrill seeking	write own scripts, engage in malicious acts, brag about exploits
insiders, user malcontents	moderate	high	disgruntlement, personal gain, revenge	uses insider privileges to attack current or former employers
coders, writers	high	moderate	power, prestige, revenge, respect	write scripts and automated tools used by newbies, serve as mentor
white hat hackers, old guard, sneakers	high	very low	intellectual gain, ethics, respect	non-malicious hacking to help others and test new programming
black hat hackers, professionals, elite	very high	very high	personal gain, greed, revenge	sophisticated attacks by criminals/thieves; may be ‘guns for hire’ or involved in organized crime
cyber terrorists	very high	very high	ideology, politics, espionage	state-sponsored, well-funded cyber attacks against enemy nations

Table 3: Selection of hacker threat actor types. Source: Meyers (et al.), 2009:8. Table 1: A Taxonomy of Cyber Adversaries

require more technological expertise or heavier use of digital technologies to penetrate than others (Gordon & Ford, 2006 in: Finklea, 2015). So, implicit in the notions of growing sophistication of attacks and capability is also the idea that these might be helping to create such a dimensions as ‘criminal career’ but also display various levels of organization. The dimension ‘group characteristics’ as element of cyber attackers is mentioned as an important dimension, especially as researchers identify a trend of increasing sophistication,

industrialization and subsequent specialization occurring in cyber crime (cf. Koops, 2010; Broadhurst et al., 2014). McGuire (2012) in Broadhurst et al. (2014) claims that “80% of cyber crime could be the result of some form of organized activity”. However, much unclarity as to the exact nature and predominance of organization in cyber crime remains (cf. Koops, 2010; Carrapico & Lavorgna, 2015). Consequently, different group characteristics (e.g. Van Hulst & Neve, 2008) and different group types (e.g. Choo, 2008; McGuire in: Broadhurst et al., 2014) need to be identified.

Examples of specific threat actor groups which have resulted in specific typologies/taxonomies are: ‘insiders’ (cf. Meyers, Powers & Faissol, 2009; Nurse et al., 2014; Nykodym, Taylor & Vilela, 2005) and ‘hackers’ (cf. McBrayer, 2013; Van Holsteijn, 2015). One of the oldest ones is Rogers’s typology (2006; 2009) which identifies different hacker types based on the dimensions ‘motivation’ and ‘skill level’, although others have subsequently added more classes to the dimension ‘motivation’ (cf. Meyers, Powers & Faissol, 2009) as can be seen in Table 3.

As one of the latest hacker typologies, Seebruck (2015) has identified a relatively simple two dimensional (‘motivation’ and ‘sophistication of attack’) method to plot the various threat actor types as can be seen in Figure 5.

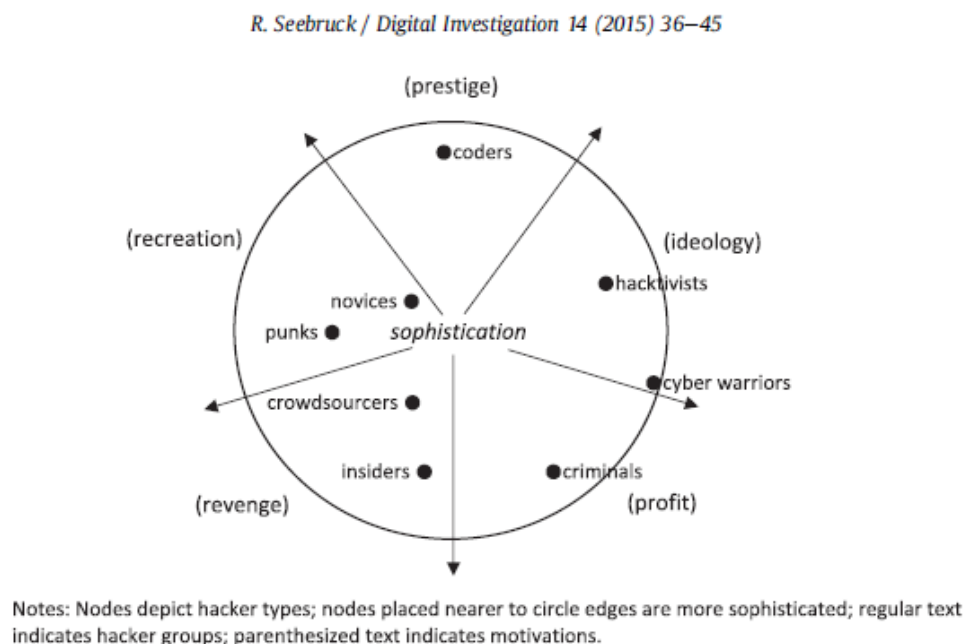


Fig. 1. A circular order circumplex of hacker types.

Figure 4: Seebruck’s threat actor dimensions. Source: Seebruck, 2015:40. Figure 1: A circular order circumplex of hacker types

These typologies again confirm that typologies in use often consist of (too) many different threat actor types but also that dimensions such as ‘motivation’, ‘skill’ and ‘level of sophistication of the attack’ and some aspect of organization more or less consistently reappear.

3.1.4 Typologies focusing on attacks on specific targets

A fourth set of typologies in literature identifies threat actor types via typologies and taxonomies of targets. For example, Gandhi et al. (2001) identify various important attack dimensions such as 'motive', 'victims', 'means of attack' and 'consequences' as can be seen in Figure 6.



Figure 5: Attack dimensions. Source: Gandhi (et al.), 2001:36-37. Figure 4: Categorization of cyber-attack dimensions

Examples of typologies of more specific attacks on targets include cyber laundering (Filipkowski, 2008), DDoS attacks (Mirkovic & Reiher, 2004), attacks on SCADA systems (Zhu & Sastry, 2011), critical infrastructures (Rege-Patwardan, 2009), cloud services (Gruschka, 2010) and high-tech crime (cf. Van Hulst & Neve, 2008). Dimensions in these typologies are often compiled via so-called profiling studies at the classification levels of attacks. Finally some authors discuss the term attack vectors (cf. Simmons et al., 2009; Choo, 2011) and analyze the threat of cyberattacks but do not relate them to actors but to the type of crime or attack.

3.1.5 Conclusion

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. Different countries employ different methods to identify threat actor types. Furthermore, many of the typologies in literature are either too generic, generating unwieldy amounts of threat actor types or focused too specific on particular attack types (e.g., DDoS attacks) or on specific classes of threat actors which focus on specific targets (e.g., SCADA systems, critical infrastructures, etc.). The majority of studies in which cyber threat actor types are identified or threat actor typologies are presented fail to provide detailed information on the classification method.

Despite these findings, which overall indicates a disheartening picture of state-of-the-art thinking on threat actor typologies, a certain common basis for building a cyber attacker typology emerges. Relatively little variation exists in a number of key dimensions, which means that the variation in the clusters of factors which describe threat actors seems fairly low. Dimensions identified in these various literatures are highly overlapping and can be synthesized in five dimensions:

1. target
2. expertise
3. resources
4. organization
5. motivation

While there is a lot of support in prior work for these five dimensions, there are often inadequately conceptualized and operationalized to identify (threat actors) in the current threat landscape. This is especially true for the dimension 'organization'. Few prior frameworks have explicitly conceptualized it. The frameworks that did, produced awkward threat actor classes. For example, Broadhurst et al. (2014) identify 6 different types of cyber criminal groups. However, as a sub-dimension, they distinguish level of online activity, and thus identify offline and online cyber criminal groups. Such a classification clearly does not suit the purpose of this research. It is important to develop a better understanding of this dimension as it has become increasingly critical to our understanding of the threat landscape. Threat actors increasingly collaborate and form larger organizations, loose networks or flexible criminal supply chains, which makes them increasingly difficult to identify as groups (cf. Mission Support Center, 2016:17; Burton, 2015). To incorporate these insights, the existing dimensions need to be developed beyond the state-of-the-art in the literature.

3.2 Operationalizing the dimensions: developing the framework

A second step in the deductive phase entails the conceptualization and operationalization of the dimensions. One of the key requirements of the method to develop the threat actor typology is that the method is replicable by security professionals. NCSC/NCTV intelligence analysts in particular are considered to use and maintain the typology in the future (WODC, 2016). To support practitioners, an intermediate product is developed that allows NCSC/NCTV analysts 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 form of the tool – a so-called cyber threat actor typology framework – is designed as a concise set of questions that supports NCSC/NCTV staff members 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. The framework is provided to illustrate the method that is developed. For example, the choice of the classes was made by the researchers with the explicit aim to reduce the number of potential threat actor classes where possible. Consequently, the choices made in the next subsections for the classification scales can be criticized. We will return to this issue in the reflection in section 5.5.

3.2.1 Target

The first dimension in the threat actor typology framework is the identification of the ‘target’, i.e. victim who owns the asset that is the target of the threat actor. In Meriam-Webster, the term target is defined as: “a place, thing, or person at which an attack is aimed.” In search for a concise, yet useful classification the initial version of the framework yielded the classes: ‘individuals’, ‘property’, ‘organizations’. However, the classification is extended to ensure that various target-types are identified. Various classes on a continuum from the individual citizen to the whole of society are subsequently identified and evaluated. In the final version of the typology framework 4 classes are identified: ‘citizen(s)’, ‘enterprise(s)’, ‘public sector’, and ‘critical infrastructure(s)’.

The second dimension was initially defined as ‘capability’, which was subdivided in three simple classes (high, medium and low). However, to allow for a finer granularity in the assessment of the capability of threat actors, this dimension is split up into the dimensions ‘resources’ and ‘expertise’. This is especially useful since this allows security practitioners and particularly NCSC/NCTV staff to make full use of available incident (scenario) data.

3.2.2 Expertise

The dimension ‘expertise’ describes what knowledge and skill level the threat actor needs to possess to plan, organize and successfully conduct the (intended) attack. Expertise is defined as: “the level of generic knowledge of the underlying principles, product type or attack methods (e.g. Internet protocols, Unix operating systems, buffer overflows).” (ISO/IEC 18045(2008):284). For the dimension skill, three simple values are provided: low, medium or high (Van Holsteijn, 2015:37). When different types of expertise are required, the range of required levels of expertise are recognized.

3.2.3 Resources

As ‘resources’, Lenin, Willemson & Sari (2014) identify such resources as ‘budget’ and ‘available time of the attacker’ (Van Holsteijn, 2015:26), which are subsequently used in the threat actor typology framework. To further aid in the classification process, a limited number of indicators are provided and ample examples in the illustrative text of the threat actor typology are provided.

The combined dimensions of ‘expertise’ and ‘resources’ allow the distinction between the various attack patterns which point towards different types of threat actors as can be seen in Table 4. Threat actors that wage attacks with low levels of expertise and are capable to mobilize large amounts of resources are able to mount DDoS attacks, just like Anonymous has been generally inferred to do (Mansfield-Devine, 2011). On the other extreme a single hacker, was thought to be singlehandedly responsible for the so-called Mirai-attacks. Employing malware, which reportedly allowed the hacker to harvest a large a botnet consisting of more than 500,000 IoT devices, these bots were used to conduct the largest DDoS attacks seen so far (Krebs, 2017). The hacker had used high levels of expertise and low levels of resources to infect millions of devices via malicious code (Pultarova, 2016).

Similarly, a low level of resource, low expertise type of attack is typically attributed to script-kiddies who use readily available exploit kits and attack old and well-known vulnerabilities. At the other extreme, one could identify attacks involving high levels of expertise and resources such as the attack on the Ukrainian electricity grid (E-ISAC, 2016; Zetter, 2016a) and the Stuxnet attack (Langner, 2011a; 2011b). It could be argued that a very different type of threat actor would be required to undertake the complex and highly resource-intensive attack on

the Ukrainian electricity grid. Not only was the level of expertise high, but also the amount of resources required for this attack could be labelled as high in that a breach was present many months before the actual event took place, allowing the attackers access to the Ukrainian grid operator systems.

The attack on the Ukrainian low-voltage electricity grid

For the first time in history hackers managed to gain control of the (low-voltage) power systems in parts of the Western Ukraine in December 2015. Although the size of the impact was small, the attack has gained notoriety as being the first physical take-over of SCADA systems affecting a vital civilian critical infrastructure. The blackout which resulted from the coordinated attacks on various infrastructure operators lasted between 1 and 6 hours and affected some 230,000 people. Post-incident analysis revealed a complex and coordinated attack-pattern, conforming an elaborate preparation, and execution of highly coordinated attacks. Although the tools used showed high expertise (e.g. sophisticated spear phishing, what really stuck was attacker's "capability to perform long- term reconnaissance operations required to learn the environment and execute a highly synchronized, multistage, multisite attack" (E-ISAC, 2016:5). Zetter (2016a) quotes an expert saying: "To me what makes sophistication is logistics and planning and operations and ... what's going on during the length of it. And this was highly sophisticated."

Stuxnet

Stuxnet, "was first reported in June 2010 by a security firm in Belarus, [and] appears to be the first malicious software (malware) designed specifically to attack a particular type of Industrial Control System (ICS)"(Kerr et al., 2010:1). It turned out to be a highly sophisticated and aggressive worm which could spread to computers that were not connected to the internet; it was highly targeted, yet was also specifically designed to remain undetected (Falliere et al., 2011; Langner 2011a; 2011b). The malware was not designed to steal information, but rather to target and disrupt control systems and disable operations. Even more specifically, Stuxnet disrupts a Microsoft Windows-based application that is employed by Siemens ICS's in nuclear facilities, particularly those of centrifuges, which enrich nuclear material. "The code's sophistication suggests that a nation state was behind the worm's development, either through proxy computer specialists or a government's own internal government and military capabilities" (Kerr et al., 2010:1). The developer had to be "financially well-resourced, employ a variety of skill sets (including expertise in multiple technology areas), have an existing foreign intelligence capability in order to gain access and knowledge of a foreign system, and be able to discretely test the worm in a laboratory setting" (Kerr et al., 2010:2).

Expertise			
Resources		Low	Medium
Low	Script-kiddie attack		Mirai-attack (2016): hacker infects millions of machines with malware
Medium			
High	Anonymous mounts DDoS attacks		Targeted attack on the Ukrainian electricity grid (2015), Stuxnet (2010)

Table 4: Expertise and resources identify different attack patterns and different threat actor types

3.2.4 Organization

The fourth dimension, ‘level of organization’, was initially operationalized in terms provided by McGuire (2012 in Broadhurst et al., 2014) who identified two sub-dimensions (‘level of organization’ and ‘level of online activity’). The resulting organizational types (swarms, hubs, clustered hybrid, extended hybrid, hierarchies and aggregate groups) however, do not seem very informative.

To increase the conceptual rigor and analytical relevance of this dimension we turn to a well-established distinction from institutional economics and governance studies: hierarchy, market, network (cf. Williamson, 1985; 1999; Bevir, 2012). This classic distinction is later extended to expressly include more loosely organized bodies such as communities and collectives, which also seem to play a relevant role in the current cyber threat landscape (Tenbensel, 2005; Alexander, 1995).

Table 5 summarizes the classes of the dimension ‘organization’. On the one extreme the collaborative form ‘hierarchy’ can be identified, which relies on “authority and centralized control” (Bever, 2012:16) to coordinate tasks. The assumption behind hierarchical forms of collaboration is the existence of a unified command structure, clear purpose, and specialization. Enforcement of authority is often “achieved by sovereignty and jurisdiction of a nation-state, by organizational control of the firm or by contractual regime. Examples include national laws and regulations, formal intergovernmental arrangements, organizational cyber security policies, or ICANN and RIR contracts, etc.” (Kuerbis & Badiei, 2017). Generally, hierarchies rely on “a rule-based approach to authority” (Bever, 2012:16), meaning a clear command and control structure, which emphasizes top-down control. The advantage of the hierarchical structure is typically that it is able to take on more complex tasks that require a lot of coordination, which is more difficult to achieve via markets or network interactions among relatively autonomous agents.

‘Networks’ can be defined as: “multiple actors who are formally separate but depend on one another for key resources and so build long-term relationships to exchange resources” (Bever, 2012:26). Network structures provide a “semi-permanent, voluntary negotiation system...[that] allows interdependent actors to opt for collaboration or unilateral action in the

absence of an overarching authority” (Scharpf, 1997; Mueller, Schmidt and Kuerbis, 2013). The rise of networks has been identified as an important trend in (cyber) criminal literature on the attack as well as the defensive side (cf. Choo, 2008; Kshetri, 2010; Broadhurst et al., 2014; Leukfeldt, 2016). Networks differ from hierarchies because they do not usually contain an authoritative command and control center to resolve disputes among the actors. Networks, instead more rely on trust across webs of associations. They differ from ‘markets’ – the next class – in that actors engage in repeated and more prolonged exchanges via coordination methods other than bargaining. Instead, they employ mechanisms such as trust to facilitate coordination and collaboration. Variations in network forms can occur with more ‘dense’ forms of networks which lean towards the more hierarchical side and ‘looser’ networks in which relationships between actors are shorter and obviously closer to the market side. Similarly interdependence in networks varies from participatory networks, where actors have roughly equal resources to ‘managed networks’ where lead actors have more resources and take on a coordinating role.

A ‘market’ is “a more or less formal arena in which goods [or services] are exchanged for other goods and especially money” (Bevir, 2012:22). Transactions among actors are primarily driven by information and price mechanism, and enforced by law and contract. Examples of markets in the realm of cyber security are “the purchase of cybersecurity consulting services, security software and equipment, zero-day markets, etc.” (Kuerbis & Badiei, 2017). Markets for cyber crime have similarly grown quickly in complexity, size and sophistication (cf. Holt, 2012; Ablon et al., 2014). Actors engage voluntarily in exchanging goods at a specific price, which is determined by their interaction. In contrast to the networks, the interactions are more “episodic” or “isolated” and “impersonal” as coordination is enabled via mechanisms such as prices and competition (Bevir, 2012:24). Consequently, markets are placed lower after networks on the dimension.

	hierarchy	network	Market	collective
coordination mechanism	authority	trust	Price	solidarity
basis of relations among members	Jurisdiction of a nation-state, organizational control of firm, contractual regime	exchange of resources	contracts and property rights	common interest
degree of dependence among members	dependent	interdependent	independent	independent
means of conflict resolution and coordination	permanent structures, rules and commands	semi-permanent structures, negotiation, diplomacy	episodic haggling, bargaining	all the means of other forms, but also voice and exit

Table 5: Coordination mechanisms in various group settings. Based on: Bevir, 2012:17. Box 1. A typology of organizational structure

Finally, as the least coordinated group, 'collectives' of individuals can be identified who engage in forms of collective action, which in turn can be defined as "all activity involving two or more individuals contributing to a collective effort on the basis of mutual interests and the possibility of benefits from coordinated action" (Marwell & Oliver, 1993 in: Agarwal, Lim & Wigand, 2011:226)(cf. Kumar, Raghavan, Rajagopalan & Tomkins, 1999:1481; Lee, Vogel & Limayem, 2003).

3.2.5 Motivation

As the fifth and final dimension, the 'motivation' of the threat actor was identified. Van Holsteijn (2015) identifies two main sources of motivation (internal and external) of threat actors, resulting in a range of sub-classes: financial benefits, causing damage, knowledge gaining, pleasure, and notoriety (cf. McBrayer, 2014). The sources of motivation were reduced to the proposed classes: 'personal', 'economic', 'ideological' and 'geo-political' to speed up the classification process. The 'personal' class contains everything a person gains from an attack except economic gain, which includes incidents from disgruntled employees and behavior such as cyber bullying, doxing people and cyberstalking. It should be noted that the classes are not mutually exclusive but can be used to characterize the dominating motivation and therefore the underlying goal of the attack of the threat actor.

3.2.6 Conclusion

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.

Any user of the typology design faces the daunting task to systematically cut back the potentially vast number of options to manageable proportions. And this should be done in a structured and controlled sense and should also be replicable over time and by different people. In short, a second and crucial step in the design of a usable threat actor typology design method would be a tool which users could use to quickly identify threat actor types and aid in the classification process. The next section discusses the reaction of stakeholders and cyber security experts on the proposed threat actor typology dimensions and classes. This information will be used to help develop such a tool, which we call a threat actor typology framework.

3.3 Feedback on the framework from experts and stakeholders

As part of the design of cyber threat actor typology semi-structured interviews were held with stakeholders and potential future users about the CSAN threat actor typology. Interviews with cyber security stakeholders such as analysts of NCSC, but also cyber security experts and (representatives of) victims of criminal behavior and cyberattacks were conducted to validate the deductively generated threat actor typology. In total 18, semi-structured in-depth interviews were held with security experts that are in a privileged position with regard to knowledge about threat actors, and that have valued perspectives on both the current CSAN actor typology, and their preferences for certain dimensions. The selection of respondents was based upon a desire to achieve overall representation of stakeholders ranging from hardware designers to software providers, IT service providers, banks, small and medium enterprises all the way to agencies engaged in cyber security who either work with the threat actor typology or play an important part or are engaged in cyber security. The selection of respondents was coordinated with the research committee. 4 representatives from critical

infrastructure industries were interviewed and a final one declined after having agreed to the interview initially, 4 experts from (inter)national cyber security companies, 2 large multinationals, 2 representatives from the banking industry, 2 representatives of industry sectors, 2 cyber security researchers and 2 finally two staff members from NCTV/NCSC. The interviews were either recorded or summarized via field notes. Respondents were provided with short minutes of the interviews. Given the sensitivity of the research topic respondents were promised anonymity to freely talk about threat actors and the threat actor typology. No information will therefore be attributable to single individuals and/or organizations. The interviews were designed in such a way that they could provide information to both the inductive and deductive cycle. Respondents were invited to share impressions about observed threat actor behavior or accumulated knowledge about trends or processes which could be linked to threat actors as well as information about the design of the threat actor typology and more specifically the threat actor typology framework. The respondents were questioned about their opinion on three generic themes; each theme is summarized in the following sub-sections and provides important information which for the design of threat actor typology.

3.3.1 Dimensions of a cyber actor typology

Respondents were first asked what threat actor characteristics they considered most relevant. Which threat actor characteristics enabled them to identify one threat actor type from the other? Interestingly many respondents started their responses by claiming that their organization did not have the capability, the resources, or the time to engage in elaborate processes of threat actor identification. Security experts added that it was almost impossible to readily identify threat actors.

One critical infrastructure company actually declined an initial positive response to the interview claiming that the progress towards a threat actor typology had not progressed to the extent that a meaningful response could be provided to the interview protocol that was sent along with a request for an interview.

However, as an important characteristic, experts from a cyber security firm, distinguished important attacks from threat actors from less important ones based on the more 'business-oriented' nature of attacks and their repetitive nature. A representative of an energy network company added that an additional important distinction to assess threat level was whether an attack was 'limited' to the cyber domain or part of a much more threatening and complex too organize mixed, coordinated physical and cyber attack. Important info the cyber security expert needed to know about incidents is: where did the attack take place and what was hit and what are the consequences for the primary process.

Many organizations such as NCSC, a multinational bank, as well as large international hard- and software providers explained how elaborate incident monitoring and analysis were of crucial importance to them to engage in attribution. To identify threat actor types thus requires a good Computer Emergency Response Team (CERT) capability as well as a good level of incident data registration. Extensive technological capabilities such as (near) real time intrusion detection systems and elaborate procedures are used to monitor threats. The representative from the large bank mentioned that acquiring this capability requires substantial investments in incident registration and monitoring.

Attribution is accomplished via analysis of the detailed technical characteristics of an attack, the so-called 'modus operandi'. When attack patterns reappear (i.e., use of the same infrastructure; similar attack pattern), the underlying toolbox of the different attackers is the same. Furthermore all attackers develop unique patterns of attack, use their own toolset and

slightly different settings. Respondents explained how advanced analysis by forensics specialists in special departments in large multinationals which develop hard- or software analyze these threats, identify threat actor attack types, and develop responses as fast as possible; for example in response to zero-day exploitations.

Representatives from various cyber security firms confirmed the limitations and approaches mentioned by representatives of so-called target organizations and argued that threat actor types were primarily identified and defined via analysis of their tools, techniques and procedures (TTPs) and the consequences of the attacks. Basically, feeding this analysis is as much information on the attacks as is possible to collect. As a consequence of this approach one international IT security firm identified four threat actor dimensions ('general, capability', 'modus operandi', 'activity'). Three of these dimensions consist of 6 classes³ resulting in 11 identified threat actor types. A representative from another internationally operating cyber security firm identified three broad threat actor types: 'activists', 'criminals' and 'nation states' and explained that his company specialized in cyber crime and subsequently identified more different and specific threat actor types based on various attack methods. The representatives of cyber security firms thus stressed the importance of a more detailed cyber threat actor typology; this also influenced their reactions to the cyber threat actor typology framework. Their focus seemed to lie primarily with specific threat actor attribution rather than actor type classification.

A senior security manager at a big European bank admitted that the company had a threat actor typology which was nearly similar to the one used in CSAN, but its role was not formally established and consequently it was applied differently throughout the organization. The respondent had inquired in the organization and found out that although a lot of information was generated about aspects related to threat actor characteristics ('modus operandi', 'threat matrices', etc.), (almost) no information was explicitly collected about cyber threat actor characteristics.

Nearly all respondents thus employed resources and extensive processes to collect empirical data which supported the identification of threat actor types based on incidents. In sharp contrast, a representative of a critical information infrastructure company found an elaborate incident reporting system largely time and resource consuming. Although the organization recognized the importance of a CERT capability, it found elaborate incident registration too complex and cumbersome to cope with the rapidly evolving threat landscape and the enormous amounts of threats. Instead, the company employed a very concise typology which consisted of three different dimensions: 'threat vector', 'motivation', and above all 'business impact'. Furthermore, the organization only identified 4 different threat actor types. The respondent explained that 'business impact' was very important as the main goal of the typology was to inform and alert executive board members about ongoing threats and keep their attention on these incidents. The small and concise typology, along with a 'light' incident and impact registration process according to the representative, enabled the critical information infrastructure company to quickly identify threat actors and to adhere to a rigorous and uniform method of communication about threat actors across the organization and especially to the executive board. Furthermore, it enabled the company to develop additional tools such as an online threat index based on number of incidents and types of

³ General (classes: Associated events, Actor type/category, Motivation, Target sector, Target geography, Intended effect; Impact effect); Capability (classes: Resources, Skills, Resolve, Access to target, Risk sensitivity, Capability score); Modus Operandi (MO)(classes: Reconnaissance activities identified, Preparation, Infiltration, Entrenchment, Compromise, Exploitation); Activity (Activity score, Date of incident (per incident)).

incidents to provide the organization and its executive members with a sense of the severity of the current situation, analogous to the public 'defcon' or terrorism alert levels.

3.3.2 Perspective on the current and proposed cyber actor dimensions

A second set of questions asked the respondents to reflect on the CSAN typology and the dimensions which were deductively identified. First off, the CSAN typology was criticized for a variety of reasons.

Some interviewees such as a critical infrastructure operator found the CSAN typology too complex and too time consuming to assess incidents and identify a potential threat actor type. A future typology would have to improve on this characteristic.

Secondly, when reviewing the list of threat actor types from the CSAN actor typology (NCSC, 2016:12, Table 1) respondents could not always explain the inclusion of threat actor types 'no actor' and 'cyber researcher' and felt these threat actor types were out-of-place in a threat actor typology. To consider 'no actor' as a threat actor type was considered paradoxical and inconsistent.

And finally, respondents responded how certain threat actor types were not visible to them. For example, a cyber security manager of a large multinational bank acknowledged that the threat actor type 'cyber researcher' was not recognized based in incident reports. A risk manager at a critical infrastructure organization argued that certain threat actor types were not considered in the risk analysis because the standard security norm for certain parts in her system was the base line information security government (BIR). This standard is designed to protect systems against threat actor types like script kiddies, hackers, etc. However, this also means that BIR means that parts of the organization are not completely protected against threat actor types such as highly skilled and resourced criminal groups, state actors or terrorists. The electricity network company IT security manager confirmed the existence of a layered defense against certain types of threat actors and argued that because of this layered defense, CSAN did not provide enough information about whether the electricity industry would need to (better) protect itself against certain threat actors and/or attack types. This in turn left the security practitioners in these critical infrastructure industries wondering when a sector or part of a sector could be considered 'sufficiently protected'. The electricity network company IT manager described how the perception of a reduced threat perception resulting from incidents in less heavily protected parts of the system could be deducted from the fact that security incidents which involved manipulation of IT and/or information in the office environment were not immediately escalated to a crisis management level; incidents that affected the technical systems were. It was argued that to really be (cap)able to inflict damage in the technical network of the electricity system required fairly specific technical expertise and knowledge of 'technical' software, which is often quite complex and old. This provided additional barriers that make it difficult for certain threat actor types to actually disrupt and damage the technical system.

The security manager of a large European bank also criticized the typology for its inability to distinguish new threat actors such as state-affiliate hacker groups. However, overall, the bank representative was of the opinion that the CSAN typology was quite complete regarding the other threat actor types and that the bank used virtually the same cyber threat actor types as the NCSC in its threat actor typology. However, he did note large differences existed between the various threat actor types. For example, hacktivists and (cyber)criminal groups were regularly recognized during incidents whereas other actor types such as nation states, terrorists, and researchers were not.

The critique that the typology did not capture recent trends in the threat actor landscape was shared by representatives of a cyber security company, a critical infrastructure expert at a research institute and a representative of the internet industry.

And finally, various respondents criticized the current actor typology and the CSAN report for being unable to aid practitioners in responding to threats and threat actors that were identified. The CSAN reports did not enable them to fully assess the dynamics and the magnitude of the trends. In short it did not provide them with a complete perspective on the threat landscape. Respondents of two critical infrastructure industries, and SME and internet industry representatives all felt the typology and CSAN reports did not provide them with the type of information they need to organize an effective response. All these respondents complained about the rather generic and high-level information provided by the incidents that were described and the generic terms in which is written about trends in the threat actor landscape. The critical infrastructure risk manager and SME representative argued for NCSC to provide more information on the threat actors. Also unclear was whether the typology and CSAN could be considered as input for risk assessment. Should the threat actors and incidents mentioned in the CSAN be considered as initial risk or residual risk in the organization's risk assessment?

However, apart from criticism, respondents also argued how despite these shortcomings, the CSAN did provide them with useful information. The critical infrastructure risk manager explained how the descriptions of incidents in CSAN were used as business impact assessment tool. Also, it provides insight in trends and indications of shifting capabilities of threat actors. However, she added, but we see this is changing very fast.

In various stages of completion, the respondents were also confronted with concepts of the threat actor typology. Respondents recognized the proposed dimensions and could provide examples of classifications with the help of the framework typology. However certain responses pointed towards the need for improvements in the typology framework, its dimensions or the classification. For example, the representative of the internet industry, when confronted with an early classification on the dimension 'organization' reacted that this dimension was perhaps not up-to-date; the dimension to him did not seem able to capture the extremely dynamic nature of the internet in terms of organizational capability. Furthermore the dimension motivation – which at that time was called 'intention', he felt, would pose difficulties as well.

The senior security manager of a large European bank pointed out that in the version of the threat actor typology framework 'internal actors' could not be identified whereas this was an important source of threats and attacks.

A cyber security expert from an international IT security firm and the senior security manager from a large European bank felt that the dimensions did not catch the essence of all the important new possibilities for behavior that the internet presented for threat actors. Additional aspects or highlights which could enhance the dimensions were the addition of information. The bank security manager argued that information on the source of origin of the attack would be an important source of information to classify an attack. In a similar fashion, the cyber security expert from an international IT security firm argued that target information such as the impact of the incident, target type/size of the intended target also yields a lot of information about the threat actor. And so would information about the visibility of the attack or more detailed information about the type of expertise (e.g. technical expertise, money laundering expertise, organizational expertise or financial expertise).

3.3.3 Cyber security incidents and trends

The respondents were finally questioned about important incidents and trends which they felt needed to be more accurately reflected in the new threat actor typology.

The electricity network company IT manager identified a trend in the thinking about cyber security where protection was moving from the 'fortress idea' towards that of a hotel with 'electronic locks' which shields important parts of the building from unwanted visitors. He and the critical infrastructure risk manager had already explained how this trend created new challenges for the interpretation of the CSAN and the use of the threat actor typology.

A representative of a cyber security company mentioned the increasing professionalization of cyber criminals and the speed in which this took place. This according to him required cyber security professionals to quickly distinguish between the various forms of cyber crime to direct resources into fighting the more dangerous and sophisticated threat actors. A security researcher also observed this trend, identifying an increased expertise and level of professionalism in the advanced phishing attacks (e.g. more sophisticated plan of attack, more resources in setting up the attack). As examples of these trends, the experts mentioned the use of personalized headings in phishing mails and the development of automated self-learning phishing mails.

Another trend that was described by the cyber security expert of international cyber security company that the motivation of certain cyber criminals was changing. Traditionally it used to be quite clear what the purpose of cyber criminals was for targets such as banks (i.e. to steal money). This led to an increasing 'sophistication' of the attacks on banks. But this is no longer the case for certain cyber criminals are displaying what he considered as 'lateral movement' i.e. new forms of attack and new cyber crime 'products' are made based for example upon from stolen bank data. The criminals are no longer focusing on stealing the money from the banks themselves. Instead, they create new 'products' which can be used in other kill chains. For example, information of bank clients is sold to other cyber criminals to improve their phishing attacks in order to gain access to computers of bank clients. Then new types of attacks can be planned: for example customer credit card fraud can become a new vulnerability. This may have consequences for the classification of the attack and threat actor classification and also has implications for the protection of assets of these potential targets such as banks.

Based on these interviews, continuous improvements were made in the threat actor typology, its dimensions and the design of classes in the threat actor typology framework.

3.4 Observations and feedback from NCSC/NCTV workshop

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. The validation was used to obtain feedback on the usability of the typology framework. Also issues that arose from using and applying the typology framework in attempts to identify threat actor types.

To achieve this goal the group deliberations were observed and recorded. The workshop consisted of a 2-hour session in which the NCSC and NCTV staff members were split up in two groups and initially asked to apply the threat actor typology framework to analyze incident descriptions which were described in the CSAN 2016 (NCSC, 2016). In a subsequent round the workshop attendants were asked to quickly identify cyber threat actors based on the review of headline incidents from the Security.NL-website in the period 15-02-

2017 until 23-02-2017). Plenary feedback rounds were held in between to collect and discuss issues that arose from the use of the framework typology with the NCSC/NCTV staff.

Among the headlines were the following links:⁴

- More smart toys made with listening function
- Privacy regulators conduct research into Windows 10
- Researchers infect BIOS/UEFI with ransomware
- Ukraine target of malware that can eavesdrop on conversations
- Germany bans smart toy because of privacy
- Shamoon-attack which deleted thousands of pc's started with macro
- Dozens of universities in the Unites States hacked via SQL-injection.

In total the analysts mapped 11 incidents using the threat actor typology framework.

On the whole, the workshop proved the viability and functionality of the threat actor typology. The workshop users generally liked the set-up of the typology framework because it raised a lot of issues about the incidents, the information provided and forced the workshop attendants to explain their analysis on the threat actor type, which in turn raised questions on the characteristics of the treat actor type. Use of the framework yielded substantial debates among participants on threat actor types in the CSAN 2016, especially the cyber researcher type (see also chapter 4).

Based upon the results of the workshop the threat actor typology framework needs to be improved, and especially additional information is required to inform users how to use the framework and search for an answer to the various questions (see Table 6).

Observation about threat actor typology use	Changes made to threat actor typology
Changing perspectives in analyzing incidents and scenarios	Additional preliminary information ('a few key points') to users of the typology framework provided calling for the development of consistent interpretation
Unclearity with regard to what constitutes a kill chain (i.e. the sequence of events that constitutes an attack)	Additional preliminary information ('a few key points') to users about how to start an analysis of an attack scenario to identify the kill chain.
Influence of time on the classification of an incident: Carbanak incident in CSAN 2016	Additional preliminary information ('a few key points') to users about the effect of more information in hindsight and its effect on classification efforts
In dimension target unclearity about the class government. How would an attack on a hospital be classified?	Change made to class from government into public sector

⁴ These headlines and the underlying messages can be found via: <https://www.security.nl/archive/>

Unclear about the meaning of various dimensions (i.e. expertise) more clear examples of what the researchers mean with the various dimensions	Additional explanation in the introduction of the dimension including examples
Insufficient (detailed) information to classify incidents on all the dimensions	Additional preliminary information ('a few key points') to users about the need to answer all questions and how to deal with insufficient information
Use of assumptions to infer information on dimensions on which no information exists	Additional preliminary information ('a few key points') to users about the need to answer all questions and how to deal with insufficient information

Table 6: Issues experienced by workshop participants and remedies

The main conclusion of the workshop was that analysts and advisors felt they were incapable of identifying a specific threat actor by filling in the cyber actor typology framework. The type of information available to the staff members based on the CSAN-report as well as the website yielded insufficient information. That is, based upon the information provided in the workshop (i.e. the descriptions in the CSAN 2016 and the 'live' examples) staff members found it hard to decide in which classes the incident would fit and thus allowed for multiple classes. Information on vulnerabilities, trends and incidents as described in the CSAN provide valuable but insufficient information to pinpoint a threat actor type and determine an exact categorization. However, in the framework introduction ('a few key points') additional information was provided to users how to deal with this perceived lack of information. The following information was provided: "The answer categories of the questions cannot be defined in precise detail, because of the complexity and dynamic nature of the threat landscape. Some degree of user discretion is necessary. We suggest that different users analyze the same threat information and then compare the outcomes, building a consistent interpretation across the user group. This is similar to developing "inter-coder reliability" in scientific research."

An important topic, which evoked further discussion was the relative judgment about incidents over time. For example, the Carbanak incident elicited discussion among analysts about the level of expertise and resources displayed in the incident. On the one hand, the expertise could be argued as medium to high since the attackers used sophisticated tools. On the other hand the workshop participants argued the incident could be ranked as medium in terms of resources since the tools used and the methods were more or less 'copied' from the successful 2016 Bangladesh Bank attack.⁵

⁵ However, as can be seen in the attack descriptions in the grey boxes, the opposite argumentation seems to make more sense: the Carbanak attacks (2013-2015) took place before the Bangladesh Bank attack (2016).

Carbanak

Carbanak refers to a group of cyber attackers, which have allegedly been held responsible for a range of attacks on financial institutions around the globe. The attacks lasted from late 2013 until 2015 and in total affected over 100 financial institutions resulting in losses amounting to more than US\$1 billion. Via spear phishing emails with infected attachments, the attackers were able to exploit vulnerabilities in Microsoft Word and Office software. This created a backdoor which was called “Carbanak”. Having gained access, the attackers were able to infect dozens of computers and install additional software on them. In this way, the attackers could reconnoiter and observe critical financial processes within these financial institutions, even using video surveillance to observe processes. Usually, this period lasted between two and four months. Actions undertaken by legitimate banking staff were observed and later meticulously copied by the attackers using existing methods, procedures and mechanisms (Kaspersky, 2015; Osborne, 2015).

2016 Bangladesh attack

On February 4 and 5 2016, attackers using malware were able to direct 35 payment requests totaling US\$951 million via the SWIFT international banking system from the Bank of Bangladesh to bank accounts in Sri Lanka and the Philippines. Using malware and hiding their requests, the attackers succeeded in avoiding a number of potential internal alerts. However, failures in the transfer requests by the attackers and suspicions raised at the US Federal Reserve allowed the authorities to recuperate many funds; only a fraction of the payments, some US\$81 million was transferred to Philippine casino accounts. As was the case in the Carbanak attack, the attackers took the time to observe and study the routines and procedures (cf. Corkery, 2016; Zetter, 2016b).

This workshop outcome about the quality of the information provided in CSAN corresponds with the interview results which concluded that the CSAN report generates valuable anecdotal evidence of potential vulnerabilities. However, in many instances insufficient information is provided in the CSAN to actually link incidents to a specific threat actor type. Instead, vital information on one or more of the dimensions of the threat actor typology could only be inferred. How could be dealt with this lack of knowledge? Consequently, both practitioners and stakeholder respondents admitted that the CSAN holds interesting information on trends and vulnerabilities, but these sources of information do not necessarily result in the identification of a specific threat actor. This problem of attribution will not be addressed in the remainder of this research.

A second related outcome of the workshop was the realization that it needed to be clearly articulated in the typology framework that the starting point of any application of the threat actor typology framework is based on an incident or an attack scenario that results in an (imagined) attack on the Dutch cyber infrastructure. Trends and vulnerabilities do not suffice as threats and therefore do not yield threat actors.

3.5 Final threat actor typology framework

Based upon the feedback from the interviews and the workshop, a final redrafting of the threat actor typology framework was undertaken. Efforts were made to make the final threat actor typology framework a concise, stand-alone document that could be used without having to read the full report behind it. This document is reprinted in its entirety on the following pages.

The typology framework can be considered as a separate product of the research. It contains an up-to-date set of key dimensions of threat actors which support quick classification of threat actors from descriptions of incidents and scenarios. The framework typology functions as a tool which enables practitioners to discuss with each other about the identification of threats, the classification of events and the analysis of incident scenarios. However, we present it here as an intermediary product and integral element of the proposed method to develop a threat actor typology. This method will be continued in the next chapter.

THREAT ACTOR TYPOLOGY FRAMEWORK

Short introduction

You have information about threats – drawn from various sources, like incidents, breach notifications, intelligence reports, and threat analysis. You want to associate these threats with a certain type of threat actor. This framework is meant to support you in this effort.

The core of the framework consists of five questions. The idea is that you use these questions to systematically characterize the threat actor that is associated with a threat that you are interested in. The questions distinguish threat actors along five dimensions: target, expertise, resources, organization and motivation. Once you have answered the questions, you will have identified a certain actor type. When this type is already present in your typology, then you are done. If not, you have ‘identified’ a new threat actor and you need to decide whether to add this new actor to the typology. This also means you have to come up with a descriptive name for the actor type.

It is important to note that the framework is not meant to address the always difficult problem of attribution. The framework assumes that the user has a scenario in mind about the attack and about who might be behind it. It merely guides the user from this scenario to a certain actor type, ensuring that this process is systematic applied to every threat and results in a consistent overall typology. In practice, of course, many threats are surrounded with unknowns. As with all threat assessment, these gaps in our knowledge will have to be filled, one way or the other, to associate the threat with a certain actor type. The gaps can be filled with anything from forensic evidence, partial incident data, expert opinion or raw speculation.

In sum, the objective of the framework is to enable the development of a more consistent and rigorous typology of threat actors for the Cyber Security Assessment Netherlands (CSAN). The dimensions were drawn from an extensive literature review and further validated via interviews with cyber security experts and stakeholders and the analysis of incident data.

A few key points before starting

- A threat actor is defined as: “an individual or conglomerate of individuals who (intend to) attack information systems which will harm the confidentiality, integrity, and availability of information (systems) in the Netherlands.”
- The starting point for classification is an attack scenario. The scenario can describe an observed or a potential attack that leads to a breach of confidentiality, integrity or availability of an asset.
- Publishing a vulnerability is in itself not a breach of confidentiality, integrity, and availability, so not a threat scenario. The researcher publishing this discovery is therefore not a threat actor, nor part of a threat actor. The exception is if a researcher actively and secretly supplies the vulnerability for the purpose of an attack, as is being done by zero-day vulnerability sellers. In that scenario, this researcher *does* become part of the threat actor.

- A threat actor comprises all those actively participating in the attack scenario (or 'kill chain'). In other words, threat actors can range from individuals to larger constellations of attackers. In order to avoid inconsistent boundaries and levels of analysis, we define as a single threat actor the whole constellation of people involved in the 'kill-chain' of the threat you are analyzing, from the entity who gives the order for the attack to the persons who execute the final steps. Answer the questions for this composite actor.
- To classify a threat agent, the entire set of questions must be answered. It will often happen that information to confidently fill in the typology is missing. In that case, assumptions have to be made. The blind spots have to be filled in. Uncertainty can also be captured by choosing a range of categories on a certain dimension, rather than a single category. Over time, with more information on certain incidents becoming available, a more precise and evidence-based classification might be possible.
- The only exception to answering the entire set of questions is when the answer category for motivation is 'unintentional'. For unintentional security incidents, there is no actual threat actor and hence no added value in completing the framework.
- The answer categories of the questions cannot be defined in precise detail, because of the complexity and dynamic nature of the threat landscape. Some degree of user discretion is necessary. We suggest that different users analyze the same threat information and then compare the outcomes, building a consistent interpretation across the user group. This is similar to developing "inter-coder reliability" in scientific research.
- Sometimes threat actors can turn out to encompass actually two (or more) different categories of a certain dimension. In principle, one could split this up further into different types of threat actors. The decision whether to further disaggregate a threat actor is a decision we leave to the analyst. It means trading off higher granularity of actor types against a keeping a manageable typology.
- Backward reasoning is possible. The dimensions in the typology framework are interdependent. For example, the target type has a certain correlation with the level of expertise and level of resources. E.g. if the attack takes place on a critical infrastructure, it could be inferred that the level of resources needed was high and medium to high-level knowledge was needed. However, it should be argued that this is working along assumptions that need to be verified per incident. Counter-intuitive cases exist. For example, script kiddies have been known to have gained access to critical infrastructures. Although it is by no means a clear relationship, these techniques might help identify threat actors more quickly.

1. Target

We start with identifying who owns the asset that is the final target of the kill chain. In principle, multiple answers are possible. The answer categories are also not mutually exclusive. Note, however, that the specific asset being targeted might suggest a specific type of owner. A threat that seeks out PLCs might be more appropriately categorized as "critical infrastructure" than as the more generic category of "enterprises".

Some attacks are so-called "untargeted", such as generic malware. In the end, however, machines with these untargeted infections are not a goal in themselves, but used in a specific kill chain, for example online banking fraud. In this example, the owner of the asset are citizens and, perhaps, enterprises.

Key question: **Who owns the asset that is targeted by the threat agent?**

<input type="checkbox"/> Citizen(s)	<input type="checkbox"/> Enterprise(s)	<input type="checkbox"/> Public Sector	<input type="checkbox"/> Critical infrastructure(s)
-------------------------------------	--	--	---

2. Expertise

The second dimension asks what knowledge and skill level the threat actor needs to possess to plan, organize and successfully conduct the (intended) attack.

To provide some guidance, it could be argued that simple DDoS attacks or defacements require low expertise. An example of a medium level of expertise would be the use of financial malware and cash-out operations in an attack on online banking, which implies a longer and more sophisticated kill chain. Finally, a high level of expertise is assumed in the well-known Stuxnet-attack (2010) or the attack on the Bangladesh Central Bank (2016).

Key question: **What level of expertise is needed to execute this (potential) attack?**

<input type="checkbox"/> Low	<input type="checkbox"/> Medium	<input type="checkbox"/> High
------------------------------	---------------------------------	-------------------------------

3. Resources

Next to expertise, it is important to assess the amount of resources that are needed in a certain threat scenario. As an indicator, one could think about the number of person months that are required or the amount of money and equipment spent in the (intended) attack from its conception to development to its final execution. Massive collective DDoS attacks by Anonymous were deliberately designed as resource extensive from the outset. Similarly, the Mirai-attacks (2016) were allegedly the product of a single hacker, requiring little resources.

On the high side of the spectrum, an example is the attack on the Ukrainian electricity grid (2015). The amount of resources required for this attack could be labelled as high as the security breach lasted months allowing the attacker access to the Ukrainian grid operator systems and ample time to observe and learn about its functioning.

Key question: **What level of resources is needed to execute this (potential) attack?**

<input type="checkbox"/> Low	<input type="checkbox"/> Medium	<input type="checkbox"/> High
------------------------------	---------------------------------	-------------------------------

4. Organization

A fourth dimension first distinguishes between individuals and larger constellations as threat actors. Next, within the larger constellations, we distinguish the type or relation between the different attackers in the kill chain.

Some constellations are loosely formed collectives or communities, such as Anonymous. They lack central hierarchy and behave swarm-like. Other constellations are brought together via market transactions, such as gamers purchasing booter services to go after

competing gamers. A third type of constellation is a network of attackers, where collaborative relationships are more stable and recurring over time. This can take different forms. One example could be that a state consistently recruits services from a certain group of cyber criminals over time to engage in state-sponsored attacks. Think of Fancy Bear working with, or at least for, the Russian authorities. The last type is hierarchy, which is a group of attackers that is vertically-integrated across the kill chain, working as a single entity, typically with a clear command structure which emphasizes top-down control. An example are actors behind the most sophisticated attacks on financial institutions. Because of the high degree of coordination needed for these attacks, all expertise is in-sourced in one close-knit group.

Key question: **How would you characterize the relationships among the attackers involved in the threat scenario ('kill chain')?**

	Constellation			
<input type="checkbox"/> Individual	<input type="checkbox"/> Hierarchy	<input type="checkbox"/> Market	<input type="checkbox"/> Network	<input type="checkbox"/> Collective

5. Motivation

Motivation is about the underlying goal of the attack. Is the attack intended or perhaps unintended such as when a USB-stick with sensitive data is accidentally lost by an employee? Is it for personal reasons such as revenge, fun or notoriety? Is it profit-driven, hence economic? Is there an ideological message or goal that is central to the incident? Or is it geo-political, trying to improve the position of a state actor viz a viz its allies, neutrals or enemies?

Key question: **How would you characterize the motivation of the threat actor?**

<input type="checkbox"/> Unintentional	<input type="checkbox"/> Personal	<input type="checkbox"/> Economic	<input type="checkbox"/> Ideological	<input type="checkbox"/> Geo-political
--	-----------------------------------	-----------------------------------	--------------------------------------	--

4 The inductive approach – data analysis

The inductive cycle allows drawing inferences about the threat actors by analyzing abuse and incident data. Analyzing the data enables certain inferences about ongoing attacks. This, in turn, sheds light on certain threat actor dimensions, as developed during the deductive phase. Think of which assets are being targeted or how many resources are being brought to bear in the attack. In other words, the data allows an improved characterization of the threat actor(s) involved in a particular cyber threat environment.

Currently, different types of cyber incident data sets can be collected and analyzed. 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
- Cyber criminal markets

In this chapter, we analyze several case studies to provide examples of how these datasets can be leveraged to feed the cyber actor typology.

4.1 Spam trap data

Email traps, more commonly referred to as spam traps, are valid email addresses that have not been used for any legitimate email or published anywhere on the Internet. In other words, they only receive illegitimate mail and spam. The main goal of a spam trap is to identify spammers or senders without data hygiene processes. Spam traps are specifically designed to identify different spam campaigns and capture spam.

By analyzing the content of the spam emails, one can glean information about the dimensions target, resources and expertise. We illustrate this in a case study of 2,230,235 emails that were captured by several spam traps deployed by third parties located across the globe. These emails contained different URLs mainly linked to phishing sites. Specifically, we captured 513,874 unique phishing URLs. Figure 7 shows the number of unique phishing URLs captured daily. As it can be seen there exists an increasing trend of this number which could be associated with an increasing number of botnets (and therefore potentially different attackers who employ phishing tactics in their attacks). This figure also shows a certain periodicity over time which is directly related with different phishing campaigns. Moreover, in 2016 the number of phishing URLs was 2 orders of magnitude higher than in 2014. This increase evidence that attackers are increasingly able to set up larger numbers of phishing sites.

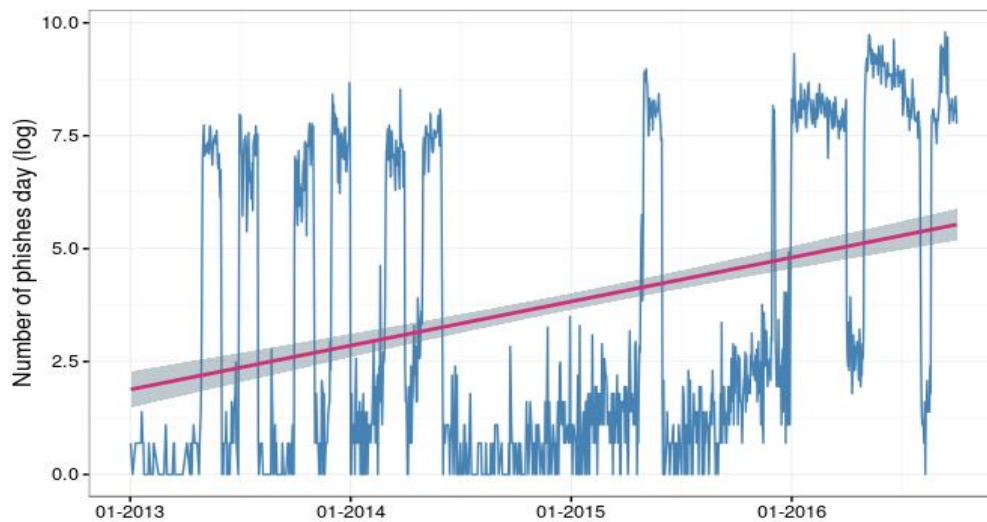


Figure 6: Evolution of the daily number of phishing URLs

By geolocating the IP addresses of the servers where the phishing sites were hosted, we can gain insights about the resources of the attackers. Figure 8 shows a heat map of the number of unique phishing URLs per country. Based on this analysis it could be concluded that America, Asia and Oceania are the continents that host the majority of the phishing sites.

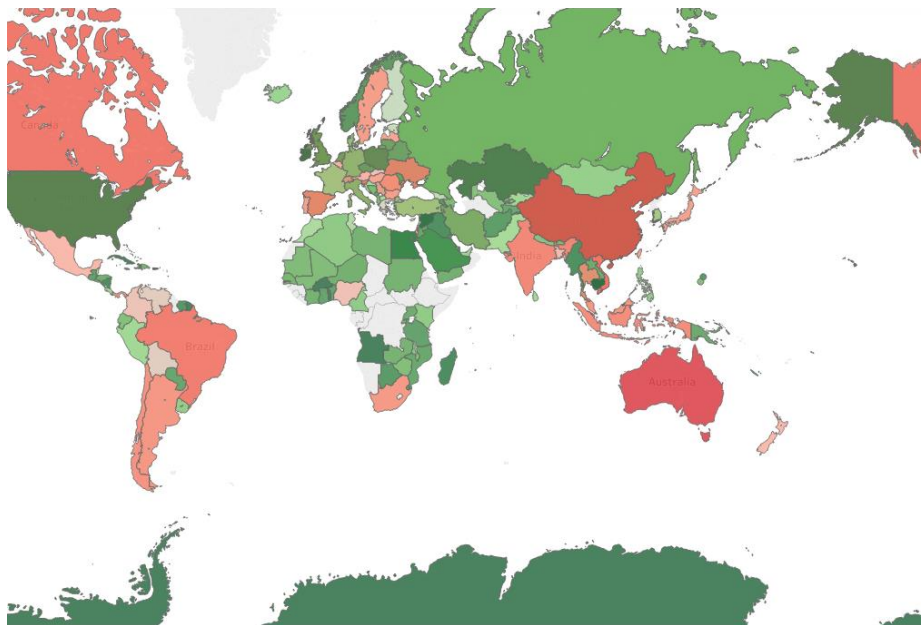


Figure 7: Map of the geolocation of the phishing URLs

Figure 9 shows the percentage of phishing URLs per country. The US by itself hosts more than 55% of the total number of phishing sites, by far the biggest number. This denotes the large number of vulnerable web servers in this country. This concentration thus allows us to understand where the resources of the attackers are mainly located.

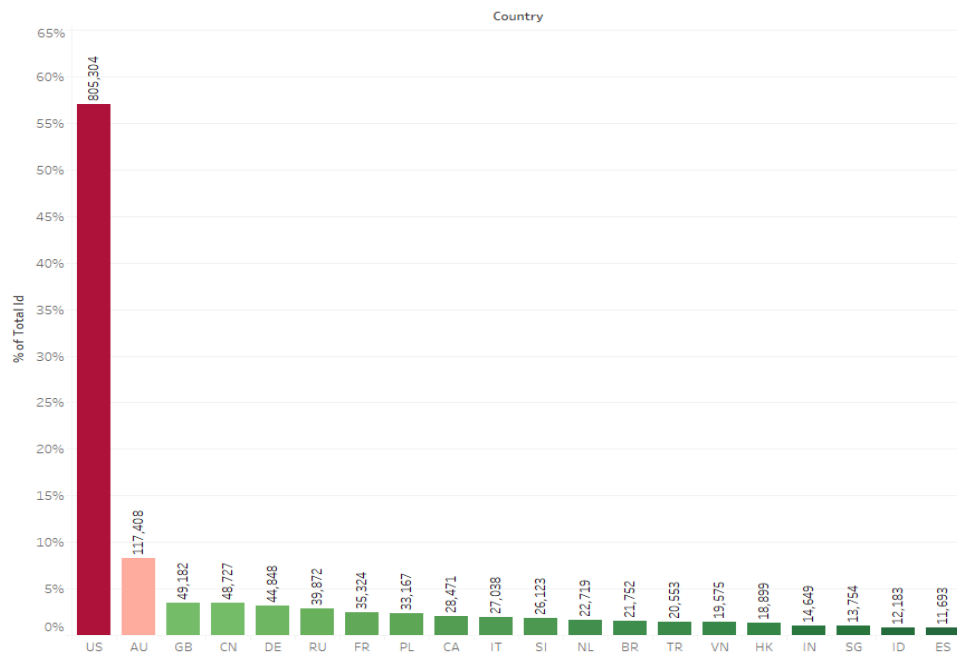


Figure 8: Percentage of the phishing sites per country

By analyzing the content of the phishing sites, we can also understand which services are mainly targeted in these attacks. Table 7 shows the services that were phished and the number of unique URLs targeting that particular service. Google and PayPal were the most targeted services during the analyzed period. From this table, it is clear that the aim of the phishing attacker is to intercept the credentials of the users of different services that could lead to financial gain by exploiting those or selling them.

Target	% Phishers	#Phishers	Target	% Phishers	#Phishers
Google	22.89%	108,218	Live	0.70%	3,318
Paypal	15.88%	75,102	RHB Banking Group	0.55%	2,602
Apple	5.63%	26,612	DocuSign	0.55%	2,588
Microsoft	5.09%	24,082	Comcast	0.49%	2,324
Wells Fargo	4.94%	23,343	Banco Do Brasil	0.46%	2,171
Sulake	4.35%	20,563	National City	0.45%	2,126
Dropbox	3.88%	18,327	HMRC	0.44%	2,084
eBay	3.20%	15,111	RBC	0.42%	2,001
Free	2.95%	13,934	IRS	0.41%	1,936
			Hotmail	0.40%	1,893
Adobe	2.64%	12,495	Santander UK	0.39%	1,834
Yahoo!	2.49%	11,767	ANZ	0.36%	1,715
USAA	2.20%	10,414	SunTrust	0.35%	1,675
Amazon	1.90%	8,987	Cariparma Credit	0.35%	1,643

Chase	1.49%	7,066	Banca di Roma	0.34%	1,628
DHL	1.24%	5,871	Barclays	0.34%	1,621
AOL	1.23%	5,813	EDF	0.33%	1,583
ATO	1.22%	5,748	Other	0.33%	1,570
Alibaba	1.16%	5,472	NAB	0.32%	1,513
AT&T	1.12%	5,317	Bradesco	0.32%	1,507
TD Canada Trust	1.10%	5,184	Westpac	0.32%	1,507
CIBC	1.02%	4,806	Smile Bank	0.30%	1,434
Facebook	0.93%	4,378	Itau	0.30%	1,398
Bank of America	0.91%	4,304	Capital One	0.25%	1,171
Orange	0.83%	3,923	Mastercard	0.25%	1,171

Table 7: Phished services

To further understand the nature of the phished services that are targeted, we can classify these according to the business area they belong to. Figure 10 shows the business type of the sites that were hosted in the phishing URLs. IT and Financial services are the most phished ones (86%). This provides additional evidence of the preference of attackers to collect the credentials of users related to these services.

In short, the analysis of spam trap data allows to capture a huge amount of phishing URLs which in turn allow us to better characterize dimensions of the cyber actors behind the attacks. In this case scenario, the attackers are clearly financially motivated and seem to target mainly individual consumers. In the conduct of their attacks the threat actors use a medium range of resources requiring low-medium expertise depending on the sophistication of the phished website. Though these data do not speak for the sophistication or the level of organization of the criminals behind the different attacks, phishing is well-known to be not just a small one-time operation. Phishing is used extensively by organized crime groups. There are gangs of phishers organized all over the world using sophisticated and elaborate schemes to steal personal information (cf. McAfee Inc., 2007).

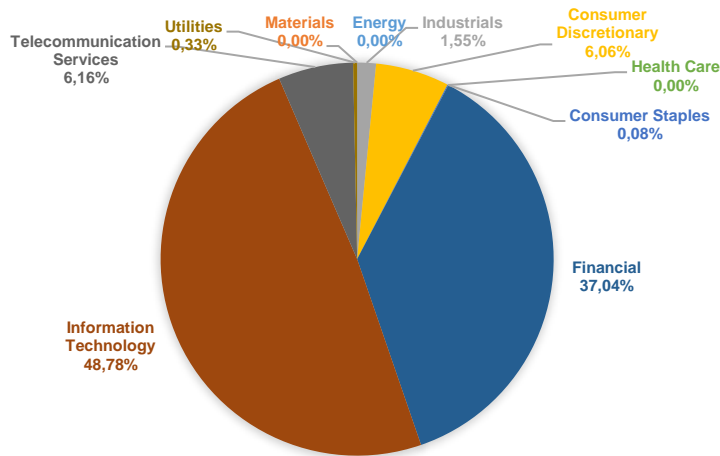


Figure 9: Business type of the phished services

4.2 Honeypot data

Honeypots allow researchers to capture different attack vectors used by threat actors by mimicking the services that are either targeted or exploited by the attackers. As a case study, we deployed 8 honeypots running services that were misused to launch amplification DDoS attacks. In particular, the services ran by our honeypots are: QotD (17/udp), CharGen (19/udp), DNS (53/udp), NTP (123/udp), SNMP (161/udp) and SSDP (1900/udp).

By analyzing the logs of the command sequences sent by the attackers to the honeypots, we can gain insights on the target and motivation of these attacks. First we can understand the volume of IP addresses targeted by the DDoS attacks. Figure 11 shows the number of IP addresses targeted by these attacks. We can see an increasing trend of DDoS attacks during the last quarter of 2015 and a more stable trend in the first quarter of 2016.

By geolocating the attacked IP addresses, we quantify the amount of attacks per country. Figure 12 plots the percentage of attacks per country. The US and China capture more than 50% of the attacks.

To gain more insights about the location of the attacked IP addresses, it makes sense to map these to the type of networks. Figure 13 shows that most of the attacked IP addresses (73%) belong to broadband networks. This reflects not only the characteristics of the attack but also the part of the motivation behind it. These attacks are not going after commercial business or critical infrastructure industries but after home users, i.e. consumers.

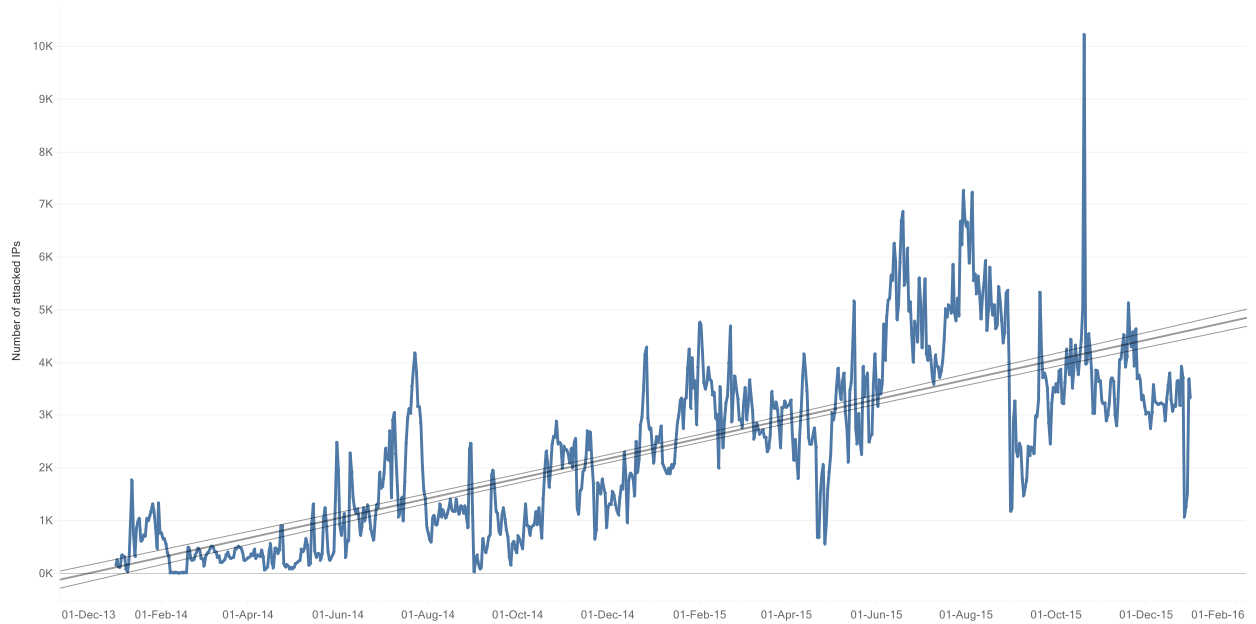


Figure 10: Number of DDoS attacks per day

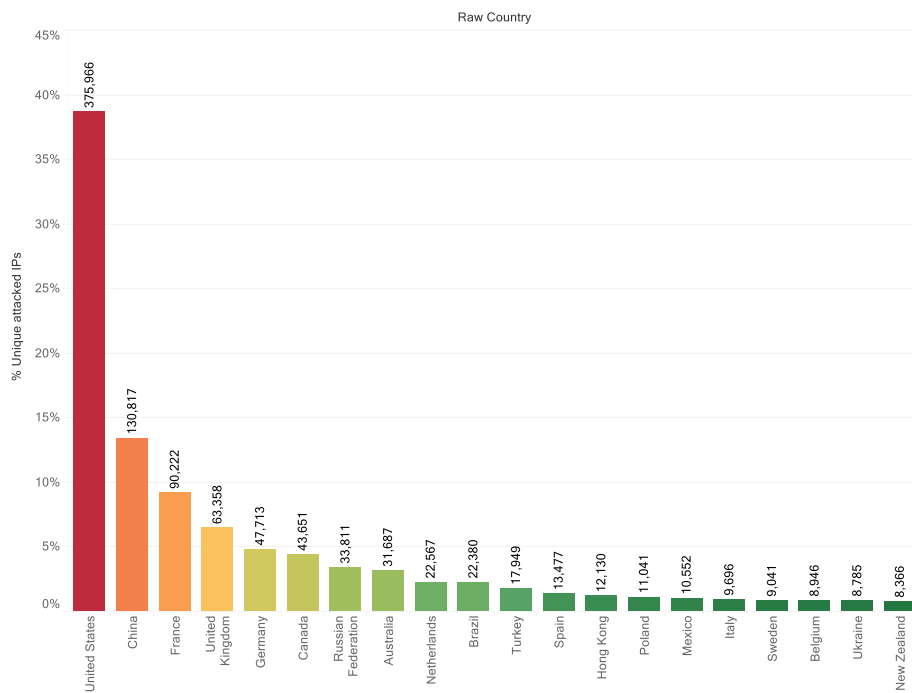


Figure 11: Number of attacked IP addresses per country

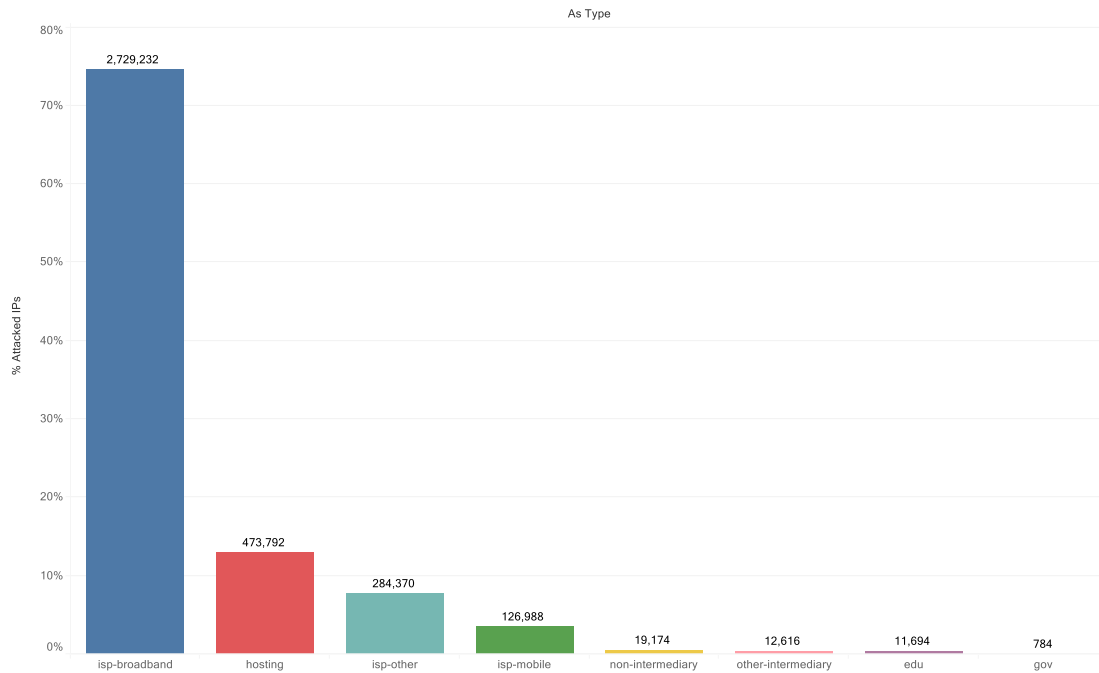


Figure 12: AS type of the attacked IP addresses

From the command sequences captured by the honeypot, we can also analyze the services that are being targeted. Table 8 shows the frequency of the attacks per attacked port. As could be expected the most attacked port is port:80, which is also the most prevalent port in internet traffic. However, it is surprising that the second most attacked ports are linked to gaming services. This also evidences the motivation of the attackers as they seem not aimed towards financial gain but just launching attacks for personal reasons.

Attacked Port	Service	# attacks	% attacks
80	http	819,242	61.68%
7000	Command and conquer	108,385	8.16%
8080	http	81,229	6.12%
27015	Steam servers	44,693	3.37%
3074	Xbox live	40,368	3.04%
1050	DNS	38,063	2.87%
2001	VideoChat	30,943	2.33%
53	DNS	24,751	1.86%
25565	Minecraft	23,926	1.80%
27005	QuakeWorld	19,666	1.48%
9987	TeamSpeak	15,988	1.20%

Table 8: Top 10 attacked ports and services

Honeypot data is rich in terms of capturing attack vectors and, thus, allows additional insights and aids in the characterization of the cyber threat actors behind these attacks. In this case scenario, the data suggests the actors behind the DDoS-attacks were medium skilled with both financial and personal motives targeting mainly consumers.

4.3 Darknet data

A darknet is a set of globally announced, but otherwise unused IP addresses. Darknet monitoring provides an effective way to observe cyber attacks that are significantly threatening network security and management. By mining darknet traffic data researchers are able to characterize the behavior of attackers and thus draw inferences on the characteristics of cyber threat actors behind them.

In the following case study, we leverage observations from a darknet of approximately 300,000 IPv4 addresses, spanning 40 networks in 15 countries to find out IoT malware propagation with Internet-wide scans. In total, we observed more than 160 billion IP packets between Jan 1, 2016 and Jan 31, 2017.

Our first step is to measure per protocol – i.e., per destination port— how many IP addresses were scanning at any moment in time. We consider a “scanner” as a host which sends at least one TCP SYN packet to the darknet. We focus on TCP, as an attacking host cannot spoof the source IP address to establish a TCP connection for exploiting vulnerable devices. In contrast, UDP and ICMP are stateless protocols and allow easy spoofing of the source IP address. To be conservative, we excluded these protocols from the measurement.

Next, we focus on the protocols where we saw a significant increase in the number of scanning hosts. This way, we follow a generic approach to discover exploitation vectors, rather than assuming particular protocols are the main vectors. A significant increase means that, for seven consecutive days, the number of scanning hosts per day reached 200 times the number that was observed on Jan 1, 2016.

Figure 13 illustrates the number of daily scanners that we identified, distinguished by the eight protocols for which we observed a significant increase: 23/TCP (Telnet), 2323/TCP (Telnet), 5358/TCP (Telnet), 5555/TCP (TR-069/TR-064), 6789/TCP (Telnet), 7547/TCP (TR-069/TR-064), 23231/TCP (Telnet), and 37777/TCP (UPnP). We manually confirmed that all of those protocols are related to IoT abuses by correlating infection attempts on these ports. This scanning behavior is directly related to IoT worms that are actively scanning these specific ports to compromise more devices. Thus, this analysis shows insight into the attacker’ resources. During peak days they own more than 2 million IP addresses related to compromised IoT devices.

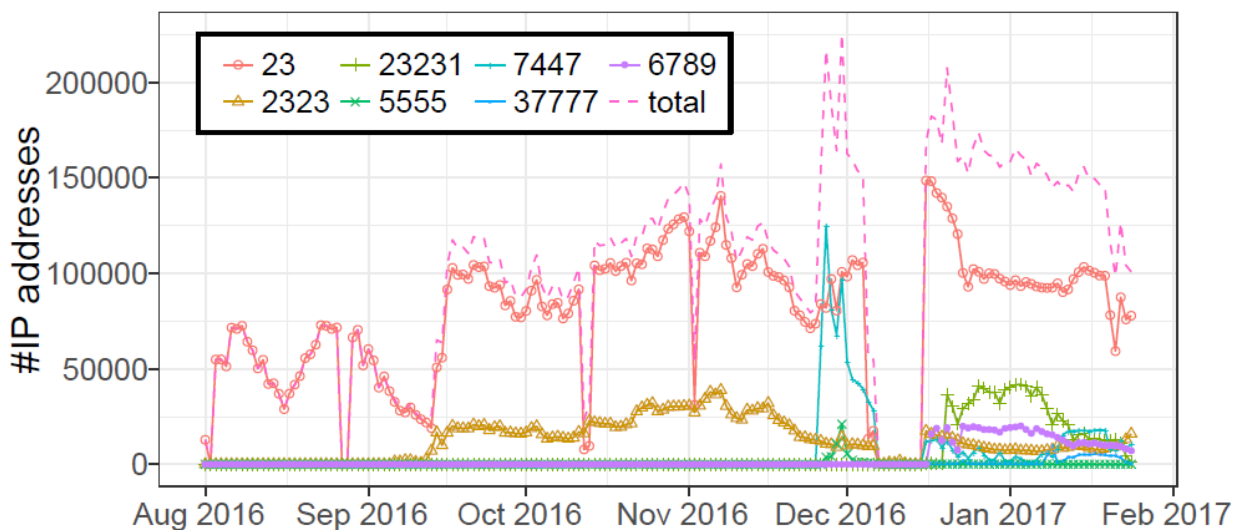


Figure 13: Number of scanning IP addresses per day

However, the analysis of darknet data does not allow the drawing of inferences about the other dimensions of our cyber threat actor typology. In this particular case study, the actors behind the scans would be cyber threat actors with low skills, targeting individual users where most of the vulnerable devices are located with both personal and for profit motives.

4.4 Cyber criminal markets

Criminal activities in cyber space are increasingly facilitated by underground black markets in both the tools (e.g. exploit kits) and the take (e.g. credit card information). These forums contain important resources for understanding cyber crime and, thus, characterizing the cyber threat actors (Portnoff et al., 2017). Depending on the type of marketplace the information contained could be used to draw inferences about all the dimensions of our typology.

As a case study, we leverage the eight distinct forums: Antichat, Blackhat World, Carders, Darkode, Hack Forums, Hell, L33tCrew and Nulled. These data are publicly available at (<http://evidencebasedsecurity.org/forums/>).

Forum	Date covered	Threads ()	%Threads for Commerce	Users
Blackhat World	Oct 2005–Mar 2008	7270	2.29%	8,718
Darkode	Mar 2008–Mar 2013	7418	27.94%	231
Hack Forums	May 2008–Apr 2015	52,649	97.34%	12,011
Hell	Feb 2015–Jul 2015	1,120	22.59%	475
Nulled	Nov 2012–May 2016	121,499	32.81%	599,085
Antichat	May 2002–Jun 2010	201,390	25.82%	41,036
Carders	Feb 2009–Dec 2010	52,188	38.72%	8,425
L33tCrew	May 2007–Nov 2009	120,560	30.83%	18,834

Table 9: Cyber criminal data users

Different forums have different purposes. For instance while Hack Forums covers a wide range of mostly cyber security-related blackhat, such as viruses, keyloggers, server “stress-testing” and hacking tools; Darkode focused on cyber criminal wares, including exploit kits, spam services, ransomware programs, and stealthy botnets.

The amount of users of each forum already evidences the popularity of these forums. To gain more insights of the products sold and bought in each forum, we apply natural language techniques to obtain the frequency of each product frequently bought and sold products.

Table 10 shows the 10 most frequently occurring keywords related to the products and services offered in Darkode and Hack Forums. Already analyzing these, we can see differences in the products sold in each marketplace. For instance, the concentration of products related to malware install and exploits is higher in Darkode than in Hack Forums where the activity around gaming cyber criminal tools is more popular. Although the motivation of the seller is always financial, analyzing the product type provides insights about the motivation of the buyer.

Products & Services	
Darkode	Hack Forums
install	account
account	service
traffic	crypter
email	space
bot	setup
root	cod
exploit	crypt
service	bot
rdp	boost
site	server

Table 10: Top 10 words used as products offered in the cyber criminal market

In summary, in the case of leveraging cyber criminal marketplaces data we can gain additional insights about the motivation of the actors (mostly profit-driven), the resources they have based on the number of transactions, and the types of product they sell (varying from high to medium skills). Indirectly, we can also learn something about the organization dimension. Certain criminal services are offered to whomever is willing to pay. This means that attack scenarios enabled with those services places the associated threat within the 'market' category, in terms of organization. It does not require the vertically integration among of criminals that is typical of hierarchy. Nor does it imply the repeated interactions and trust relations of network organization.

5 A tentative new threat actor typology

In the previous chapters the two cycles that provided the building blocks for the development of the new threat actor typology were described. The final step is the creation of the tentative new typology.

5.1 Key features of the method to develop a threat actor typology

Before we create the new tentative typology, it is important to summarize the key requirements and choices which were made in the design of the method to develop a threat actor typology so far. These issues are also explained in the standalone version of the framework (see Section 3.5).

- A threat actor is defined as an actor who (intends to) “adversely affect the reliability and security of information and information systems” in the Netherlands (NCSC, 2016:25).
- The research goal is to develop (a method to develop) a new threat actor typology that supports the reliable and efficient identification and classification of threat actors and the resulting threat actor landscape.
- The method captures key characteristics of all (potential) threat actors in a small set of dimensions to identify a threat actor type based on the available data or assumptions on each of the dimensions.
- Five key threat actor dimensions are identified: target, expertise, resources, organization and motivation.
- For each threat actor dimension classes are identified to distinguish between various actor types.
- A so-called cyber threat actor typology framework is created to help future users to classify an incident or an attack (scenario) and identify a certain threat actor type.
- The framework does not address, nor solve the problems inherent in attribution. Gaps in information have to be filled in with assumptions. Uncertainty can also be captured by choosing a range of categories on a certain dimension, rather than a single category.
- The framework typology assumes an observed or potential attack scenario – in other words, an actual breach of the confidentiality, integrity or availability of an asset. Publishing a vulnerability is not a breach and the researcher publishing this discovery is therefore not a threat actor, nor part of a threat actor. If a researcher actively and secretly supplies a vulnerability for the purpose of an attack, as is being done by

zero-day vulnerability markets, then this researcher does become part of the threat actor.

- A threat actor comprises all those actively participating in the attack scenario (or 'kill chain'). In other words, threat actors can range from individuals to larger constellations of attackers. In order to avoid inconsistent boundaries and levels of analysis, we define as a single threat actor the whole constellation of people involved in the 'kill chain' of the threat you are analyzing, from the entity who gives the order for the attack to the persons who execute the final steps. Answer the questions for this composite actor.
- To classify a threat agent, the entire set of questions must be answered. It will often happen that information to confidently fill in the typology is missing. In that case, assumptions have to be made. The blind spots have to be filled in. Uncertainty can also be captured by choosing a range of categories on a certain dimension, rather than a single category. Over time, with more information on certain incidents becoming available, a more precise and evidence-based classification might be possible.
- The only exception to answering the entire set of questions is when the answer category for motivation is 'unintentional'. For unintentional security incidents, there is no actual threat actor and hence no added value in completing the framework.
- The answer categories of the questions cannot be defined in precise detail, because of the complexity and dynamic nature of the threat landscape. Some degree of user discretion is necessary. We suggest that different users analyze the same threat information and then compare the outcomes, building a consistent interpretation across the user group. This is similar to developing "inter-coder reliability" in scientific research.
- Sometimes threat actors can turn out to encompass actually two (or more) different categories of a certain dimension. In principle, one could split this up further into different types of threat actors. The decision whether to further disaggregate a threat actor is a decision we leave to the analyst. It means trading off higher granularity of actor types against a keeping a manageable typology.
- Backward reasoning is possible. The dimensions in the typology framework are interdependent. For example, the target type has a certain correlation with the level of expertise and level of resources. E.g. if the attack takes place on a critical infrastructure, it could be inferred that the level of resources needed was high and medium to high-level knowledge was needed. However, it should be argued that this is working along assumptions that need to be verified per incident. Counter-intuitive cases exist. For example, script kiddies have been known to have gained access to critical infrastructures. Although it is by no means a clear relationship, these techniques might help identify threat actors more quickly.

5.2 Application: combining the deductive and inductive cycles

With the findings from both cycles the research has generated the maximum amount of information about key characteristics of threat actors and incident data in a structured process. The final step is the compiling of a complete threat actor typology. 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 provided

in the CSAN 2016 (NCSC, 2016). Information in the CSAN about tools, trends and vulnerabilities was distinguished from information about specific incidents and categorized in separate columns. In total, CSAN 2016 provided information about roughly 50 different trends, vulnerabilities, attacks and attack scenarios which could be used to feed the threat actor typology framework. In some instances, insufficient information could be found in the CSAN to allow for the identification of a threat actor. For example, because CSAN only described a trend, and not an attack (scenario). In other instances one or multiple potential threat actors could be identified.

However, more important than the amount of threat actors that were identified is the process through which a threat actor typology is developed. A key step in the development of a threat actor typology forms the intermediate categorization based upon the available information.

So how did this work in practice? An excerpt is shown in Figure 15 which identifies the various types of information which are provided in CSAN 2016. CSAN describes information on tools and trends for attacks; CSAN identifies vulnerabilities. And finally, CSAN identifies an attack (scenario). The table makes a systematic distinction between the various types of information in CSAN on incidents or a particular attack (scenario).

The first line of the table shows that on page 17 information CSAN signals an increasing level of targeted ransomware attacks; a trend. A vulnerability that is associated with the trend of targeted ransomware attacks in the CSAN describes how employees can be targeted in the initial phase of these ransomware attacks. The ransomware is often hidden in links in spam-mails which are sent to private e-mail addresses from employees. In many enterprises employees use private e-mail in their workplace. Attackers use this vulnerability to infiltrate enterprise networks. After having gained access attackers can proceed to the next step in their attack which aims to extort enterprises. However, a specific threat (i.e. an actual attack or scenario) is not provided in CSAN. The vulnerability was described in generic terms. Consequently, this description does not produce a threat actor type. However, the vulnerability can be clearly labelled in terms of motive and type of attack. We have labelled the description as: 'targeted ransomware attack' and since the dominating motive for the use of ransomware attacks is economic, we have coined the vulnerability 'targeted ransomware cyber criminals'.

However, CSAN also provides information on two specific attacks on hospitals in Germany and the United States (NCSC, 2016:17/18) where ransomware attacks had occurred (only one of these is shown in Table 13). The information provided in CSAN 2016 about the incidents mentions that the attack used 'normal' consumer ransomware—indicating an untargeted attack using the vulnerability described. All these bits of information, when fed into the threat actor typology framework, produce as threat actor '(un)targeted ransomware cyber criminals'.

page number	column	tool/trend	vulnerability	threat (scenario)	dimension 1: target	dimension 2: expertise	dimension 3: resources	dimension 4: organization	dimension 5: motivation	intermediate: threat actor type
17	1 and 2	targeted ransomware infection	Organisations find that ransomware infections still occur largely because workers read their private e-mail at their workplace. For this, workers use the web mail functionality of their private e-mail. In this e-mail, there are, for example, links to a website that infects the computer of the employee.	targeted ransomware infection						targeted ransomware cybercriminals
17/18 and 1	and 2	changing nature of ransomware infections		A hospital in the German city of Neuss was the victim of ransomware that encrypted patient information, as was announced in February 2016. The malware, 'normal' consumer ransomware, was distributed via an e-mail attachment. Operations had to be postponed and e-mail communication was suspended. RP Online, a German news website, stated that five other German hospitals kept it to themselves that they had incurred the same infection.	Citizen(s), Enterprise(s), Government, Critical Infrastructure	low	low	individual, collective/community, market, network	Economic	untargeted ransomware cybercriminals

Figure 14: CSAN 2016 threat actor analysis

As a final example, CSAN mentions another trend: Dutch organizations are the victims of DDoS extortion campaigns (NCSC, 2016:26, column 2). Although using a different ploy, the attack type is similar and so is the motive. If such an attack were to occur, one would categorize the attacker in the same threat actor type. These attacks are undertaken to extort victims for financial gain. And so we identified a separate threat actor: extortionists.

5.3 A first version of a new threat actor typology

Using the available information from the inductive cycle and the CSAN 2016, and clustering the various attack types and motives in an intermediate step, in a similar fashion as in section 5.2 the following threat actor types were identified.

- extortionists
- information brokers
- crime facilitators
- digital robbers
- scammers and fraudsters
- crackers
- insiders
- terrorists
- hacktivists
- state actors
- state-sponsored networks

5.3.1 Using the framework typology to plot threat agents on the typology dimensions

For each threat actor type, and each (conceivable) attack scenario, the framework typology can be used to classify the threat actor into 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 can be found in Table 11 on the next page.

5.3.2 Extortionists

CSAN 2016 provides ample information about the use of various attacks and scenarios in which cyber criminals employ extortion. In fact CSAN's key finding is that ransomware "is commonplace and has become more advanced" (NCSC, 2016:11). Based upon this information it is possible to quickly answer the questions in the typology framework. The widespread coverage of ransomware and DDoS attacks is something which is supported in CSAN. Not only citizens and enterprises are affected. Hospitals, schools, government, and even critical infrastructure industries such as the energy industry and water management organizations are in fact regularly attacked via (un)targeted ransomware (NCSC, 2016:17). Extortionists (could) thus plausibly target all classes in this dimension of our framework typology. Expertise among the attackers to engage in extortionist attacks are judged as low to medium. The fast growing, widespread and largely untargeted use of this mode of attack and the warning of the sophistication trend leads one to assume primarily low but also medium levels of expertise. On the dimension resources, the assessment would be that the amount of resources required to conduct an extortion attack is low to medium. On the organizational dimension the threat actor type would be a hierarchy, market or network. And finally the motivation would be considered either personally or economically driven.

5.3.3 Information brokers

Information brokers are threat actors who trade (stolen) information in the world of cyber crime. Examples mentioned in CSAN 2016 (NCSC, 2016:27/31) are services which are marketed in the form of medical data, stolen credit card information, social media information and e-mail account information. Multiple examples were identified in CSAN 2016 such as the watering hole attacks (NCSC, 2016:38 column 2). The targets of these threat actors could be citizens, enterprises and the public sector. The level of expertise involving attacks which seek information can range from medium to high especially when it concerns for example information on zero days or other unique but valuable 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 11: Threat actor typology based on CSAN 2016

The amount of resources need to obtain information and data via an attack can be classified as low to medium. The tools to obtain these sources of information are readily available. On the organizational dimension the threat actor type could be classified as hierarchy, market or network. And finally the motivation is economic.

5.3.4 Crime facilitators

Crime facilitators are threat actors who provide technical support to the attacks of other criminal actors. The criminal group harnessing the Dyre-malware campaign was identified as such group (NCSC, 2016:26 column 2). Facilitation can take on different forms such as the renting of botnets by so-called botnet-herders or the development of Remote Access Tools (RATs) or exploit kits (NCSC, 2016:40-41). Targets can be citizens, enterprises and the public sector. The expertise to development new tools is steadily rising and could be assessed as medium to high. The amount of resources needed to develop these tools and services is classified as medium. For example RATs are considered “labor intensive” (cf. NCSC,2016:18 column 2). The organizational constellation that characterizes crime facilitators are markets and networks. And finally the motivation is economic in nature.

5.3.5 Digital robbers

CSAN 2016 reported attacks on (financial) enterprise(s). The threat actors who target financial services attack citizens as well as enterprises. Attacks on such financial institutions are economically motivated. The threat actors display a medium to high level of expertise in their attacks. For example, the Carbanak attack gained access to the SWIFT network (NCSC, 2016:18 column 2) using a sophisticated and long kill chain. The amount of resources available also are classified as medium to high. Some of the recent successful bank attacks involved multiple attackers and required months of preparation and execution. The organizational constellation is network based.

5.3.6 Scammers and fraudsters

Scammers and fraudsters employ social engineering in their attacks on targets. The targets are citizens, enterprises and the public sector. CSAN 2016 reported spoofing attacks in the transportation sector (NCSC, 2016:18 column 2). The level of expertise needed for these types of attacks is classified as low to medium and the level of resources also low to medium. The organizational constellations which are associated with these attacks are individual, market or network. The motivation is economic.

5.3.7 Crackers

CSAN in its trends identifies an increasing threat from what is called “cyber vandals and script kiddies” because of “the growing availability of accessible tools for digital attacks (CSAN, 2016:29 column 2).” Crackers are threat actor types that seem motivated by fun (pranking) and the possibility to display their capabilities which indicate personal motives. Targets of these particular threat actor types can range from public to private enterprises and include critical infrastructures. CSAN actually mentioned DDoS attacks as particular attack scenario and reported attacks against Ziggo and the Volkskrant (NCSC, 2016:2). Expertise levels are considered low to medium as accessibility of easy-to-use and potentially destructive tools increases. The amount of resources these threat actor types have at their disposal is considered low. Motivation is personal for relatively young and brazen youngsters who are destroying for fun. Crackers tend to be relatively older and operate individually or in loosely organized collectives or networks.

5.3.8 Insiders

CSAN 2016 reported: "Although, in the recent period, some reports were published abroad about deliberate actions by internal actors, this was not such a problem in the Netherlands" (NCSC, 2016:30 column 1). However, the threat actor type is still considered a likely potential threat actor type. Insiders target organizations in which they are working which can be either public or private enterprises. The level of expertise can vary from medium to high in case of highly experienced and long-serving employees. The amount of resources available for attacks could be classified as low. The motivation of insiders can be classified as personal, economic or ideological.

5.3.9 Terrorists

CSAN 2016 (27 column 2) reports that no actual attacks of this threat actor type have been identified. However, given the persistent threat, CSAN has chosen to identify this threat actor type already and the new typology follows this example. Conceivable attacks would be attacks on enterprise(s), public sector or critical infrastructure(s). This attack requires high levels of expertise and would require medium to high levels of resources. Terrorists would typically employ the organizational constellations market or hierarchy to coordinate their attacks. Motivation would be ideological. A lack of data and experience with this threat actor group actually means that this category is less well described.

5.3.10 Hacktivists

Interestingly, many of the incidents, attacks and trends described in CSAN 2016 with reference to terrorism (NCSC, 2017:27 column 2) would qualify for this threat actor type. The level of expertise employed in these attacks is low to medium. Hacktivists are ideologically motivated but instead of operating in markets or under hierarchical leadership, hacktivists are more loosely organized either individually or in collectives or networks. Examples in CSAN 2016 were regular defacements (NCSC, 2016:21 column 1) and the attacks on the European Space Agency (ESA)(NCSC, 2016:30 column 1). But also the doxing examples undertaken by attackers who claim allegiance to terrorist organizations (NCSC, 2016:27 column 2) could be considered in this threat actor type. This way, the terrorism category is 'reserved' for other attack types.

5.3.11 State actor

This threat actor group constitutes the old fashioned, secretive and behind-the-scene attacks in which state actors target enterprises, the public sector or critical infrastructures to gain access to strategic information. Although no clear examples were provided, CSAN 2016 explicitly warns about increased levels of espionage (NCSC, 2016:21 column 1). The level of expertise and resources involved in these attacks is considered medium to high and the available resources for the attack medium to high. The constellation used to undertake these attacks is hierarchical and the motivation is geopolitical.

5.3.12 State-sponsored network

This threat actor type covers recent attacks of state-affiliated groups which are organized in networks. CSAN 2016 mentions an attack on a German-Dutch defense company by a Chinese hacker group (NCSC, 2016:19 column 2) and the Shadow Broker group attack (NCSC, 2016:20 column 2). Also the attack on the Ukrainian electricity grid is attributed to such a group (NCSC, 2016:21 column 1). These groups have suspected ties to state actors. Targets include citizens, enterprises, public sector and critical infrastructures. The level of expertise displayed by this threat actor type varies between medium and high. The amount of resources medium or high, given the

fact that the attacks which have been witnessed are considered long-term campaigns. The organizational constellation displays network characteristics and the motivation can be classified as ideological.

5.4 CSAN 2016 typology and new threat actor typology compared

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 (NCSC, 2015; 2016). A summary in which the major differences are highlighted is provided in Table 12.

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 12: CSAN 2016 typology and new threat actor typology compared

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.

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 typology, which identifies various subtypes in the horizontal lines (NCSC, 2016:12 Table 1). 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 different 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 (e.g. HPE, 2016:7). 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. However, 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.

5.5 Reflection and some final thoughts

Now that we have presented our threat actor typology a short reflection on the intended goals and the achieved result is possible. The research set out to develop a new method to develop a threat actor typology. The method was aimed to be more transparent and features a structured way to classify threat actors. The method also was designed so that it could be repeated over time.

Although the typology framework and the complete description of the complete typology design cycle could be criticized based on the choices made, a more transparent and structured process now can be identified behind the proposed threat actor typology. However, whether the typology is considered easily replicable of course remains to be seen. With the design of the typology framework, special attention has been paid to ensure practical applicability of the new method, but as always practice makes perfect. That is, continuous use of the typology by intelligence analysts and security practitioners and repetitious evaluation of the method are advised.

As was already considered in section 2.4, the end result of the study would always be a balance between the various design criteria which are inherent in typology designs.

For example, one of the most important choices to be made by typology users is to decide on the trade-off between level of aggregation and the level of exclusivity that can be reached in the typology. The researchers have made a conscious choice to keep the amount of threat actor types as low as possible to increase the usability of the typology by NCSC staff. That is, the usability requirements necessarily impact the level of detail in which various threat actor groups can be identified. Specific IT security companies for example boast much more detailed threat actor types. The addition of dimensions and classes can achieve a similar result for the new threat actor typology without sacrificing the method of the typology design.

The downside of this design choice is that the distinctive character between the various threat actor types is reduced because of this. In other words. Criticasters would argue that the current typology does not provide an exhaustive distinction between different threat actor types, as can be seen in Table 11. This in turn hinders the classification process. More detailed characterizations of threat actor types such as scammer and fraudsters would enable the distinction between different threat actor types such as scammers focusing on citizens using 'simple' phishing tools. These attacks and threat actor types can be distinguished from far more professional threat actors types who use more complex and sophisticated attacks on SMEs for example. Users and stakeholders should actively make a choice whether additional detail is a valid requirement for the new typology. The criticism and reactions from stakeholders on the current CSAN can be used as input in this discussion.

Furthermore, a number of limitations remain to be discussed. First of all, the researchers would like to stress to only allow specific data, i.e. an attack (scenario) to fill the typology.

A second limitation of the design is the fact that usability will improve after consequent and substantive use. To increase the reliability of the typology, future users should take care to ensure the requirements inherent in typology use: that of inter-coder reliability. This is a challenge in itself in a complex and dynamic world of cyber security and due care should be taken to invest in this particular aspect when the typology design is going to be used.

A third limitation in the current design is that the typology was intentionally made without making use of classifications in use by practitioners in the cyber security industry. One of the ways in which the typology could be improved is to align the typology framework to standardized classifications that are already in use in cyber security. For example, another way of classifying the dimension 'resources' would be to use the ISO-definition for resource: "equipment required to identify or exploit a vulnerability". The ISO standard identifies four sub-classes (ISO 14085:286) instead of the three in this report.⁶ Similar choices could be made with regard to the dimensions 'skill' or 'level of expertise'. Another scale identifying not three but four classes could be used based on ISO 18045 norms (2008:284-285).⁷ One of the (potential) and big drawbacks of doing so, however, would be the increased the number of classes. Users of the typology should continuously discuss and debate on the relative merits of concise versus more uniform or elaborate classes to classify incidents or threat actor types.

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.

The question of course presents itself what constitutes a 'complete' or a 'sufficiently complete' threat actor typology and how often the typology would need to be updated. The quality of the threat actor typology lies in the trading off of various criteria. Based upon the CSAN report and the input from respondents and quantitative data the new typology would ideally be updated periodically. So the challenge of the 'completeness' of the model lies in the ability of NCTS/NTCV staff to satisfactorily

⁶ The classes are: "Standard equipment, which is readily available to the attacker, either for the identification of a vulnerability or for an attack"; Specialised equipment [which] is not available to the attacker, but could be acquired without undue effort [...], or development of more extensive attack scripts or programs"; "Bespoke equipment, which is not readily available to the public as it may need to be specifically produced (e.g. very sophisticated software), or because the equipment is so specialised that its distribution is controlled, possibly even restricted. Alternatively, the equipment may be very expensive." And finally "Multiple Bespoke" refers to instances where "different types of bespoke equipment are required for distinct steps of an attack."

⁷ The classes identified in the ISO norm are: Laymen: "unknowledgeable compared to experts or proficient persons, with no particular expertise"; proficient persons, "knowledgeable in that they are familiar with the security behaviour of the product"; Experts, who are "familiar with the underlying algorithms, protocols, hardware, structures, security behaviour, principles and concepts of security employed, techniques and tools for the definition of new attacks, cryptography, classical attacks for the product type, attack methods, etc. implemented in the product or system type." And finally, Multiple expert who combines "different fields of expertise [...] required at an Expert level for distinct steps of an attack."

classify all incidents and assess which incidents cannot be (easily) mapped. The periodical parsing of (historical) incident data sets through the threat actor typology framework might achieve two goals at the same time.

First of all, working with the threat actor typology framework and achieving consistent interpretation across different users requires experience and frequent use.

Secondly, the periodical parsing of (historical) incidents through the threat actor typology framework signals the need for a new development cycle of the threat actor typology.

One of the outcomes of the research is that much information that is collected by NCSC and is provided in the CSAN actually refers to vulnerabilities and trends and much less to concrete threats and threat actors.

The prospect of more precise information on threat actor types is a luring perspective. However, many stakeholders argued that according them improvement of the threat actor typology is not a goal in itself. The real challenge which faces NCSC/NCTV is how the knowledge that is gained with the threat actor typology and the CSAN is going to be used in the future. If the new typology would succeed in providing a more rigorous and more accurate threat perspective and a clearer focus on specific threat actors, users of CSAN would very much like to receive more help from NCSC/NCTV to deal with those specific threats. A first step in this process might be to use the typology as a starting point for a discussion about critical threat actors.

Bibliography

- Ablon, L., Libicki, M.C., and Golay, A.A. (2014). *Markets for Cybercrime Tools and Stolen Data. Hackers' Bazaar*, Santa Monica: RAND
- Agarwal N., Lim M., Wigand R.T. (2011). Collective Action Theory Meets the Blogosphere: A New Methodology. In: Fong S. (eds) *Networked Digital Technologies*. NDT 2011. *Communications in Computer and Information Science*, vol 136. Springer, Berlin, Heidelberg
- Alexander, E.R. (1995). *How organizations act together, Interorganizational Coordination in theory and practice*. Luxembourg: Gordon and Breach Publishers
- Aston, M., McCombie S., Reardon B., and Watters P. (2009). *A Preliminary Profiling of Internet Money Mules: An Australian Perspective*. Cybercrime and Trustworthy Computing: Brisbane.
- Bailey, K. D. (1994). *Typologies and taxonomies: an introduction to classification techniques* (Vol. 102). Thousand Oaks: Sage
- Bennett, A., & Elman, C. (2006). Qualitative research: Recent Developments in Case Study Methods. *Annual Review of Political Science*, 9(1), 455-476. doi:10.1146/annurev.polisci.8.082103.104918
- Bevir, M. (2012). *Governance, A very short introduction*. Oxford: Oxford University Press
- Broadhurst, R., Grabosky, P., Alazab, M., Bouhours, B., & Chon, S. (2014). Organizations and Cybercrime: An Analysis of the Nature of Groups Engaged in Cyber Crime. *International Journal of Cyber Criminology*, 8(1), 1-20
- Burton, J. (2015). NATO's cyber defence: strategic challenges and institutional adaptation, *Defence Studies*, 15:4, 297-319, DOI: 10.1080/14702436.2015.1108108
- Caltagirone, S., Pendergast, A., & Betz, C. (2013). *The diamond model of intrusion analysis*. Hanover: US Department of Defense, Center for Cyber Threat Intelligence and Threat Research
- Canbolat, M. & Sezgin, E. (2016). *Is NATO ready for a cyberwar?* (MA thesis). Monterey, California: Naval Postgraduate School
- Carrapico, H., & Lavorgna, A. (2015). Space Oddity? Exploring Organised Crime Ventures in Cyber Space. *European Review of Organised Crime*, 2(2), 1-5.
- Casey, T. (2007). *Threat Agent Library Helps Identify Information Security Risks Intel White Paper*. Intel Corporation.
- Casey, T., Koeberl, P., & Vishik, C. (2011). Defining Threat Agents: Towards a More Complete Threat Analysis. In N. Pohlmann, H. Reimer & W. Schneider (Eds.), *ISSE 2010 Securing Electronic Business Processes: Highlights of the Information Security Solutions Europe 2010 Conference* (pp. 214-225). Wiesbaden: Vieweg+Teubner
- Choo, K.-K. R. (2008). Organised crime groups in cyberspace: a typology. *Trends in Organized Crime*, 11(3), 270-295. doi: 10.1007/s12117-008-9038-9
- Choo, K.-K. R. (2011). The cyber threat landscape: Challenges and future research directions. *Computers & Security*, 30(8), 719-731. doi: <http://dx.doi.org/10.1016/j.cose.2011.08.004>
- Clinard, M. B., Quinney, R., & Wildeman, J. (1994). *Criminal Behavior Systems. A typology* (3rd ed.). London: Routledge
- Corkery, M. (2016). Hacker' \$81 million sneak attack on world banking, in: *New York Times*, April 30, <https://www.nytimes.com/2016/05/01/business/dealbook/hackers-81-million-sneak-attack-on-world-banking.html>
- De Kock, P. (2014). *Anticipating criminal behaviour*. (PhD. thesis). Tilburg: Tilburg University. Retrieved from [https://pure.uvt.nl/portal/en/publications/anticipating-criminal-behaviour\(535864f8-d666-46d5-a203-15a2348e952e\).html](https://pure.uvt.nl/portal/en/publications/anticipating-criminal-behaviour(535864f8-d666-46d5-a203-15a2348e952e).html)
- Doty, D. H., & Glick, W. H. (1994). Typologies As a Unique Form Of Theory Building: Toward Improved Understanding and Modelling. *Academy of Management Review*, 19(2), 230-251. doi: 10.5465/amr.1994.9410210748

- Electricity information sharing and analysis Center (E-ISAC)(2016). Analysis of the Cyber Attack on the Ukrainian Power Grid. Washington DC: NERC,
http://www.nerc.com/pa/CI/ESISAC/Documents/E-ISAC_SANS_Ukraine_DUC_18Mar2016.pdf
- Falliere, N., Murchu, L.O., and Chien. E. (2011). *W32.Stuxnet Dossier*, Version 14 (February 2011). Cupertino, Symantec Security Response, via:
https://scadahacker.com/library/Documents/Cyber_Events/Symantec%20-%20Stuxnet%20Dossier%20v1.4.pdf, May 31, 2017.
- Filipkowski, W. (2008). Cyber Laundering: An Analysis of Typology and Techniques. *International Journal of Criminal Justice Sciences*, 3(1), 15
- Finklea, K. M., & Theohary, C. A. (2015). *Cybercrime: conceptual issues for congress and US law enforcement*. (R42547). Washington: Congressional Research Service, Library of Congress
- Fox-Brewster, T. (2017). Did Russia Hack Macron? The evidence is far from conclusive. In: *Forbes*, May 8, <https://www.forbes.com/sites/thomasbrewster/2017/05/08/macron-emails-leaked-and-russia-is-the-chief-suspect/#4f59618268f4>
- Gandhi, R.A., Sharma, A., Mahoney, W., and Laplante, P.A. (2011). Dimensions of cyber-attacks: cultural, social, economic, and political, in: *IEEE Technology and Society Magazine* 30(1):28-38. Doi:10.119/MTS.2011.940293
- Govcert.nl (2011). *Cybersecuritybeeld Nederland. December 2011* [in Dutch]. Ministry of Security and Justice: The Hague, <https://www.ncsc.nl/binaries/content/documents/ncsc-nl/actueel/cybersecuritybeeld-nederland/cyber-security-beeld-nederland/2/Cyber%2BSecurity%2BBeeld%2B2011.pdf>
- Groll, E. (2016). Did Russia Knock Out Ukraine's Power Grid?, in: *Foreign Policy*, <http://foreignpolicy.com/2016/01/08/did-russia-knock-out-ukraines-power-grid/>, May 31, 2017.
- Gruschka, N., & Jensen, M. (2010). *Attack Surfaces: A Taxonomy for Attacks on Cloud Services*. Paper presented at the IEEE CLOUD
- Gundel, S. (2005). Towards a new typology of crises. *Journal of Contingencies and Crisis Management*, 13(3), 106-115. doi: 10.1111/j.1468-5973.2005.00465.x
- Hacquebord, F. (2017). *Two Years of Pawn Storm. Examining an increasingly relevant threat*. TrendLabsSM Research Paper, Irving :Trend Micro,
<https://documents.trendmicro.com/assets/wp/wp-two-years-of-pawn-storm.pdf>
- Hallman, R., Bryan, J., Palavicini, G., Divita, J. and Romero-Mariona, J. (2017). IoDDoS — The Internet of Distributed Denial of Service Attacks - A Case Study of the Mirai Malware and IoT-Based Botnets. In *Proceedings of the 2nd International Conference on Internet of Things, Big Data and Security (IoTBDs 2017)*, 47-58,
https://www.researchgate.net/profile/Roger_Hallman2/publication/316455478_IoDDoS_-_The_Internet_of_Distributed_Denial_of_Service_Attacks_A_Case_Study_of_the_Mirai_Malware_and_IoT-Based_Botnets/links/58ff2ae6a6fdcc8ed50d93ab/IoDDoS-The-Internet-of-Distributed-Denial-of-Service-Attacks-A-Case-Study-of-the-Mirai-Malware-and-IoT-Based-Botnets.pdf
- Higgins, A. (2017). Maybe Private Russian Hackers meddled in election, Putin says, in: *New York Times*, June 1, <https://www.nytimes.com/2017/06/01/world/europe/vladimir-putin-donald-trump-hacking.html>
- Holsteijn, R. van (2015). *The motivation of attackers in attack tree analysis* (Master thesis). Delft: TU Delft
- Holt, T.J. (2012). Examining the Forces Shaping Cybercrime Markets Online. In: *Social Science Computer Review* 31(2), 165 – 177. doi: 10.1177/0894439312452998
- HPE (2016), *HPE Security Research Cyber Risk Report 2016*,
https://www.thehaguesecuritydelta.com/media/com_hsd/report/57/document/4aa6-3786enw.pdf
- Hulst, R. C. van, & Neve, R. J. M. (2008). *High-tech crime, soorten criminaliteit en hun daders. Een literatuurinventarisatie*. Meppel: Boom Juridische Uitgevers

- Jahankhani, H. & Al-Nemrat, A. (2012). Examination of Cyber-Criminal Behaviour. *International Journal of Information Science and Management (IJISM)*, 41–48.
- Johnson, T. A. (Ed.). (2005). *Forensic Computer Crime Investigation*. Boca Raton: CRC Press
- Kaspersky (2015). *Carbanak APT. The great bank robbery*. Version 2.1 Moscow,
https://securelist.com/files/2015/02/Carbanak_APT_eng.pdf
- Kerr, P.R., Theohary, C.A., and Rollins, J. (2010). *The Stuxnet Computer Worm: Harbinger of an Emerging Warfare Capability*, R41524, Washington D.C.: Congressional Research Service.
<http://nsarchive.gwu.edu/NSAEBB/NSAEBB424/docs/Cyber-040.pdf>, June 1, 2017.
- Kharouni, L. (et al.)(2014). *Operation Pawn Storm. Using decoys to evade detection*. Irving: Trend Micro, <https://www.trendmicro.de/cloud-content/us/pdfs/security-intelligence/white-papers/wp-operation-pawn-storm.pdf>
- Koops, E. J. (2010). The internet and its opportunities for cybercrime. In M. Herzog-Evans (Ed.), *Transnational Criminology Manual* (Vol. 1, pp. 735-754). Nijmegen: Wolf Legal Publishers
- Krebs, B. (2017). *Who is Anna-Senpai, the Mirai Worm Author?*, in:
<https://krebsonsecurity.com/2017/01/who-is-anna-senpai-the-mirai-worm-author/>
- Kshetri, N. (2010). *The Global Cybercrime Industry. Economic, Institutional and Strategic Perspectives*. Heidelberg :Springer.
- Kuerbis, B. and F. Badieli (2017). *Mapping the cybersecurity institutional landscape*, paper presented at 'Who Governs? States or Stakeholders? Cybersecurity and Internet Governance. Third Annual Workshop Internet Governance Project', Georgia Tech School of Public Policy, Atlanta, May 11-12.
- Kumar, R., Raghavan, P., Rajagopalan, S., & Tomkins, A. (1999). Trawling the Web for emerging cyber-communities. *Computer Networks*, 31(11–16), 1481-1493. doi:
[http://dx.doi.org/10.1016/S1389-1286\(99\)00040-7](http://dx.doi.org/10.1016/S1389-1286(99)00040-7)
- Langner, R. (2011). Cracking Stuxnet, a 21st-century cyber weapon [Video file]. Retrieved from https://www.ted.com/talks/ralph_langner_cracking_stuxnet_a_21st_century_cyberweapon, May 29, 2017
- Langner, R. (2011a). Stuxnet: Dissecting a Cyberwarfare Weapon, in: *IEEE Security & Privacy* 9(3), 49-51. Doi: 10.1109/MSP.2011.67
- Lee, F. S. L., Vogel, D., & Limayem, M. (2002). Virtual community informatics: what we know and what we need to know. *Paper presented at the Proceedings of the 35th Annual Hawaii International Conference on System Sciences*, 7-10 Jan.
- Lenin, A., Willemson, J., & Sari, D.P. (2014). Attacker profiling in quantitative security assessment based on attack trees. In 19th *Nordic Conference on Secure IT Systems (NordSec 2014)* (pp. 199-212). Springer International Publishing, DOI: 10.1007/978-3-319-11599-3_12
- Leukfeldt, E.R. (2016). *Cybercriminal Networks. Origin, Growth and Criminal Capabilities* (Ph.D. dissertation). The Hague: Eleven International Publishing.
- Lindqvist, U., & Jonsson, E. (1997). How to systematically classify computer security intrusions. In *Proceedings. 1997 IEEE Symposium on Security and Privacy* (Cat. No.97CB36097) (pp. 154–163). IEEE Comput. Soc. Press. doi:10.1109/SECPRI.1997.601330
- Luijijf, E. (2012). Understanding Cyber Threats and Vulnerabilities. In J. Lopez, R. Setola & S. D. Wolthusen (Eds.), *Critical Infrastructure Protection: Information Infrastructure Models, Analysis, and Defense* (pp. 52-67). Berlin, Heidelberg: Springer Berlin Heidelberg.
- Luijijf, E., Besseling, K., & Graaf, P. de (2013). Nineteen national cyber security strategies. *International Journal of Critical Infrastructures*, 9(1-2), 3-31. Doi: 10.1504/ijcis.2013.051608
- Mansfield-Devine, S. (2011). Anonymous: serious threat or mere annoyance?, in: *Network Security* 1(1), 4-10.
- Marinos, L. (2013). *ENISA Threat Landscape Report 2013, Overview of current and emerging cyber-threats*. Heraklion: European Union Agency for Network and Information Security
- Marinos, L. (2014). *ENISA Threat Landscape Report 2014, Overview of current and emerging cyber-threats*. Heraklion: European Union Agency for Network and Information Security
- Marinos, L. (2016). *ENISA Threat Landscape 2015*. Heraklion: European Union Agency for Network and Information Security

- McAfee, Inc. (2007). *Whitepaper. "Identity Theft"*. January 2007. URL: <http://www.pubblicaamministrazione.net/file/whitepaper/000042.pdf>
- McBrayer, J. (2014). *Exploiting the digital frontier: hacker typology and motivation* (Master thesis). Tuscaloosa: University of Alabama
- Meyers, C., Powers, S., & Faissol, D. (2009). *Taxonomies of Cyber Adversaries and Attacks: A Survey of Incidents and Approaches*, LLNL-TR-419041, Lawrence Livermore National Laboratory. <https://e-reports-ext.llnl.gov/pdf/379498.pdf>
- Mirkovic, J., & Reiher, P. (2004). A taxonomy of DDoS attack and DDoS defense mechanisms. *SIGCOMM Comput. Commun. Rev.*, 34(2), 39-53. doi: 10.1145/997150.997156
- Mission Support Center (2016). *Cyber threat and vulnerability analysis of the U.S. Electric Sector. Mission Support Center Analysis Report*. Idaho National Laboratory, <https://info.publicintelligence.net/INL-CyberThreatsElectricSector.pdf>
- Mueller, M., Schmidt, A. and Kuerbis, B. (2013). Internet Security and Networked Governance in International Relations, *International Studies Review* 15(1), 86-104
- National Cyber Security Centre (NCSC)(2012). *Cyber Security Assessment Netherlands. CSBN-2*. The Hague
- National Cyber Security Centre (NCSC)(2015). *Cyber Security Assessment Netherlands 2015 (CSAN 2015)*. The Hague: Ministry of Security and Justice
- National Cyber Security Centre (NCSC)(2016). *Cyber Security Assessment Netherlands 2016 (CSAN 2016)*. The Hague: Ministry of Security and Justice
- Noroozian, A., Korczyński, M., Gañan, C. H., Makita, D., Yoshioka, K., & van Eeten, M. (2016). Who Gets the Boot? Analyzing Victimization by DDoS-as-a-Service. In F. Monrose, M. Dacier, G. Blanc & J. Garcia-Alfaro (Eds.), *Research in Attacks, Intrusions, and Defenses*: 19th International Symposium, RAID 2016, Paris, France, September 19-21, 2016, Proceedings (pp. 368-389). Cham: Springer International Publishing.
- Noroozian, A., Korczynski, M., TajalizadehKhoob, M. & Van Eeten M. (2015) "Developing Security Reputation Metrics for Hosting Providers." In *8th Workshop on Cyber Security Experimentation and Test (CSET 15)*. USENIX Association. <https://www.usenix.org/conference/cset15/workshop-program/presentation/noroozian>
- Nurse, J. R. C., Buckley, O., Legg, P. A., Goldsmith, M., Creese, S., Wright, G. R. T., & Whitty, M. (2014, 17-18 May 2014). *Understanding Insider Threat: A Framework for Characterising Attacks*. Paper presented at the 2014 IEEE Security and Privacy Workshops (SPW)
- Nykodym, N., Taylor, R., & Vilela, J. (2005). Criminal profiling and insider cyber crime. *Digital Investigation*, 2(4), 261-267. doi: <http://dx.doi.org/10.1016/j.diin.2005.11.004>
- Osborne, C. (2015). Carbanak hacking group steal \$1 billion from banks worldwide. *ZDNet*, February 16, <http://www.zdnet.com/article/carbanak-hacking-group-steal-1-billion-from-banks-worldwide/>
- Perlroth, N. (2017). Russian Hackers who targeted Clinton appear to attack France's Macron. In *New York Times*, April 24, visited online: <https://www.nytimes.com/2017/04/24/world/europe/macron-russian-hacking.html>
- Police City of London (2016). *Cyber Crime - Victimology Analysis*. <https://www.cityoflondon.police.uk/news-and-appeals/Documents/Victimology%20Analysis-latest.pdf>
- Portnoff, R. S., Afroz, S., Durrett, G., Kummerfeld, J. K., Berg-Kirkpatrick, T., McCoy, D., ... & Paxson, V. (2017). Tools for Automated Analysis of Cybercriminal Markets. In *Proceedings of the 26th International Conference on World Wide Web* (pp. 657-666). International World Wide Web Conferences Steering Committee
- Pultarova, T. (2016). Webcam hack shows vulnerability of connected devices, in: *Engineering & Technology* 11(11), 10. Doi:[10.1049/et.2016.1112](https://doi.org/10.1049/et.2016.1112)
- Pushpakumar, H. (2015). *Understanding the threat landscape in e-government infrastructure for business enterprises* (MA-thesis). Delft: Delft University of Technology

- Rege-Patwardan, A. (2009). Cybercrimes against critical infrastructures: a study of online criminal organization and techniques. *Criminal Justice Studies*, 22(3), 261-271. doi: 10.1080/14786010903166965
- Robinson, N., Gribbon, L., Horvath, V., & Robertson, K. (2013). Cyber-security threat characterisation. A rapid comparative analysis. *Prepared for the Center for Asymmetric Threat Studies (CATS), Swedish National Defence College, Stockholm*. Cambridge: RAND Europe
- Rogers, M. (2003). The role of criminal profiling in the computer forensics process. *Computers & Security*, 22(4), 292-298. doi: [http://dx.doi.org/10.1016/S0167-4048\(03\)00405-X](http://dx.doi.org/10.1016/S0167-4048(03)00405-X)
- Rogers, M. K. (2006). A two-dimensional circumplex approach to the development of a hacker taxonomy. *Digital Investigation*, 3(2), 97-102. doi: <http://dx.doi.org/10.1016/j.diin.2006.03.001>
- Seebruck, R. (2015). A typology of hackers: Classifying cyber malfeasance using a weighted arc circumplex model. *Digital Investigation*, 14, 36-45. doi: <http://dx.doi.org/10.1016/j.diin.2015.07.002>
- Sheldon, J. (2012). State of the Art: Attackers and Targets in Cyberspace. *Journal of Military and Strategic Studies*, 14(2), <http://jmss.journalhosting.ucalgary.ca/jmss/index.php/jmss/article/view/462/458>
- Simmons, C., Ellis, C., Shiva, S., Dasgupta, D., & Wu, Q. (2009). *AVOIDIT: A cyber attack taxonomy*. University of Memphis.
- Tenbenschel, T. (2005). Multiple modes of governance: Disentangling the alternatives to hierarchies and markets, *Public Management Review* 7(2): 267-288
- Tennakoon, H. (2011). *The Need for a Comprehensive Methodology for Profiling Cyber-Criminals*, in: <http://www.newsecuritylearning.com/index.php/feature/150-the-need-for-a-comprehensive-methodology-for-profiling-cyber-criminals>.
- Warikoo, A. (2014). Proposed Methodology for Cyber Criminal Profiling. *Information Security Journal: A Global Perspective*, 23(4-6), 172-178. doi: 10.1080/19393555.2014.931491
- Wetenschappelijk Onderzoek (WODC). 2016. "Categorisering en motieven cyber actoren." <https://www.wodc.nl/onderzoeksdatabase/2740-categorisering-en-motieven-cyber-actoren.aspx?cp=44&cs=6778>.
- Williamson, O.E. (1985). *The Economic Institutions of Capitalism*. New York: Free Press
- Williamson, O.E. (1999). *The mechanisms of governance*. Oxford: Oxford University Press
- Zetter, K. (2016a). Inside the Cunning, Unprecedented Hack of Ukraine's Power Grid, in: *Wired*, March 3, 2016. <https://www.wired.com/2016/03/inside-cunning-unprecedented-hack-ukraines-power-grid/>, Retrieved May 31, 2017.
- Zetter, K. (2016b). That insane, \$81M Bangladesh Bank heist? Here's what we know, in: *Wired*, May 16, 2016. <https://www.wired.com/2016/05/insane-81m-bangladesh-bank-heist-heres-know/>, retrieved June 5, 2017.
- Zhu, B., Joseph, A., & Sastry, S. (2011, 19-22 Oct. 2011). *A Taxonomy of Cyber Attacks on SCADA Systems*. Paper presented at the Internet of Things (iThings/CPSCoM), 2011 International Conference on and 4th International Conference on Cyber, Physical and Social Computing.