Examining and Constructing Attacker Categorisations — an Experimental Typology for Digital Banking

Caroline Moeckel
Royal Holloway, University of London
Egham, UK
caroline.moeckel.2012@live.rhul.ac.uk

ABSTRACT

In this paper, we propose the experimental construction of a new attacker typology grounded in real-life data, using grounded theory analysis and over 200 publicly available documents containing details of digital banking related cybercrime and involved attackers. The current state of this research area is introduced briefly, highlighting current issues and shortcomings. This is supported by a brief investigation into the mechanisms of the construction of previous taxonomies and typologies. Eight attacker profiles forming the typology specific to the case of digital banking are presented. A short discussion of contributions made and suggestions for future research directions in this field are also added.

CCS CONCEPTS

• **Security and privacy** → *Web application security*; *Human and societal aspects of security and privacy*;

KEYWORDS

attackers, threat agents, categorisation, typology, taxonomy, threat modelling, grounded theory, digital banking

ACM Reference format:
Caroline Moeckel. 2019. Examining and Constructing Attacker Categorisations — an Experimental Typology for Digital Banking. In *Proceedings of 14th International Conference on Availability, Reliability and Security (ARES 2019), Canterbury, United Kingdom, August 26–29, 2019 (ARES '19),* 7 pages.
DOI: 10.1145/3339252.3340341

1 INTRODUCTION

Attacker analysis and profiling have long been part of the analytical toolkit of investigators and date back centuries [19], both for planning defence strategies and to aid forensics post-attack. Researchers have been interested in finding out more about the individuals behind cybercrime since the first illegal activities were observed in the early beginnings of the cyber era, initially in the area of telecommunications. In this context, attacker typologies and taxonomies are commonly used vehicles to represent attacker types and categories applicable to either a specific system or for generic usage.

ARES '19, Canterbury, United Kingdom

DOI: 10.1145/3339252.3340341

Early research in this area (e.g. [11][16][9][21]), mostly based on relatively small numbers of interviews, documented case studies and anecdotes, indicated variations amongst attackers, for example their technical skills, motives or level of damage done to the system targeted. Such observations ultimately lead to the creation of attacker categories, e.g. like the three types of computer criminals (crackers, criminals, and vandals) identified by the FBI in 1997 [14]. More recent works include the widely referenced work by [24] from 2006, with nine attacker types and a two-dimensional matrix visualisation aligning attacker motivations and resources. Based on a literature analysis of previous works on attacker taxonomies, individual hacker categories and subcategories, [18] in 2009 then consolidated research efforts to date into eight common categories of attackers. In 2012, [10] carefully updated known attacker categories, using current terminology and threat properties. More recently, in 2015, [25] proposed an updated attacker typology. While closely built on the mentioned earlier works, it has been adapted with the intent to capture "the recent increases in ideologically and socially motivated hacking". A comprehensive and critical assessment of the state of attacker typologies and taxonomies can also be found in the 2017 work by [7].

While they certainly provide interesting and accessible visualisations of human threat actor landscapes, attacker typologies and taxonomies suffer from a range of limitations and shortcomings at this point in time, with [7] concluding on "a disheartening picture of state-of-the-art thinking on threat actor typologies" after their initial literature review. For them, problems are mostly methodological, with used data sources, classification and construction methods not adequately accounted for. In our opinion, many taxonomies seem to be build on each other, reference previous literature rather than using independent real-life datasets (e.g. [18][10]), with one of the key references in the area [23] not meeting certain standards (clear publication date and route, named data sources and methodology). Additionally, we would like to add the lack of justification, rationale and purpose for many typologies and taxonomies: it is largely unclear how these can be used in e.g. threat modelling processes, what their practical benefits are for designing security countermeasures in organisations and lastly, how they can be validated.

In this paper, we propose the experimental construction of a new attacker typology grounded in data, using grounded theory analysis of over 200 publicly available documents containing details of digital banking related cybercrime and involved attackers. This is supported by a brief investigation into the mechanisms of the construction of previous taxonomies and typologies. Eight attacker profiles forming the typology specific to the case of digital banking are presented, followed by a brief note on potential improvements to this study and general future directions of research in this field.

2 BACKGROUND

To help prepare the construction of the attacker taxonomy for digital banking as presented in the remainder of this document, this background section will present strategies for building taxonomies previously used by others as well as common classification criteria and attacker types in existing taxonomies or typologies. Initially, a note on the terminology used in this research area is provided, with particular focus on the distinction between the concept of a taxonomy or typology.

2.1 Common terminology in the field

Attacker categorisations in literature use a number of terms for their various elements, starting with differing labels for the classified subjects. Many older categorisations [16][11] and the ones building closely on [24] use the term 'hacker' (e.g. [25][10] or 'cracker' in [14]), while newer propositions use more abstract terms such as cyber adversaries [18], threat agents [13] or actors [7]. Similarly, we suggest the usage of the neutral, all-encompassing term 'attacker'.

Secondly, there seems to be a split between the usage of the terms typology and taxonomy to describe the classification framework, with little reflection on why one was chosen over the other. While categorisations referring to [24] have maintained the usage of 'taxonomy' (e.g. [18][10]), latest efforts have reflected more criticially on this and suggested the use of 'typology' as more fitting. The two terms can be clearly distinguished, with [22] stating that "conceptually developed configurations are defined as typologies, while empirically derived configurations are defined as taxonomies". [25] support this by viewing taxonomies as categorising "dimensions based on empirical observation and measurable traits". In direct contrast, typologies which can be viewed as a non-exhaustive, "conceptually derived interrelated sets of ideal types" [7] p.9).

For the purpose of the introduced categorisation of digital banking attackers, we suggest the adoption of the term 'typology' following the reasoning that the categorisation is likely to be non-exhaustive and present ideal summaries of attacker groups rather than present truly empirical, in-depth and formally measurable attacker characteristics from a complete, finite dataset.

2.2 Previously used construction strategies

How have attacker categorisations then be built in the past? Early categorisation efforts have often used personal observations from a professional context (like in [9] or [14]), but also relied, consolidated and extended strongly on previous literature [24][18]. Even newer categorisations like [10] and [25] have not introduced new data to the area, but used existing web resources to review the previously employed terminology. Similarly, [25] uses literature to explain the shift in emphasis for their typology to more ideologically and socially motivated attackers. [7] have introduced a systematic hybrid approach, using both a deductive approach based on a literature review and an inductive approach, e.g. through reviewing data on cyber incidents and monitoring of ongoing attacks. Several advantages can be identified for following such an approach, like the identification of new and emerging threats and attackers as well as the removal of potential bias or methodological issues from previous studies.

For the proposal in this paper, a similar approach is suggested in Section 3, with an initial literature review (limited in the context of this short paper) followed by the analysis of a dataset on digital banking related incidents to build the categorisation.

2.3 Previously used categorisation criteria

Taxonomies aiming to label and categorise hackers and cybercrime attackers should take a certain perspective to identify variations within the entire population. One or multiple criteria are used as a lens to distinguish attackers characteristics and behaviours and to help build clusters of similar attackers which can be viewed as an attacker group or type.

Motivation (also under motives, drivers and intents) and resources (alternatively labelled as skills) can seen as major two criteria for past attacker categorisation [24][16][27][15][18][10][17][25]. Motivations may be of financial nature or based on revenge, curiosity or notoriety, but can also be found in cause and ideology. Resources or skills may refer to factors such as time and finances available to the attacker, technical skill and capabilities of the attackers, but also fewer tangible features such as initial access options or insider knowledge and personal connections available to the attacker.

Less frequently used criteria for classifications include for example the level of danger posed by an attacker or amount of damage caused to a specific system, group of users or individual users (e.g. in [5][2][11]). The methods employed to attack a system ('modus operandi') can also be used as classification criterion — [10] employ a set of threat properties in their taxonomy which includes this dimension, a view supported in [5] and [2]. Other observed criteria include moral value and judgement [26], ethical development and maturity [9], own traceability [27] as well as the attacker's attitude to risk [20]. Group structures and affliations may also be part of an attacker taxonomy [20][15].

2.4 Common attacker types

Similar to the exercise undertaken in [18], this section presents a heavily consolidated view of common attacker types across previous taxonomies and typologies. This overview should be seen as a non-exhaustive, high level indication of the range of existing attacker types found in literature.

Novices — Attackers with limited technical skills and other resources motivated by curiosity and thrill seeking can be found in most categorisations (e.g. in [16][23][24][25][10][3][5][2]).

Browsers & cyber punks — Attackers with low to moderate skill levels, funds and resources make up this group — their motivations however may slightly differ, from 'students' viewing breaking into and studying a system as an intellectual challenge [16][11] to 'cyber-punks' or 'pranksters' (e.g. in [23][25][18] describing attackers motivated by thrill seeking and possibly revenge, but also personal gain (through minor fraud activities).

Ethical hackers — Relatively consistent and well-defined cluster across several categorisations (e.g. in [5][23][24][17][10][25][18]) — highly skilled individuals defined through their intact moral code, ethics and ideology driven by passion and intellectual challenge, but with no regular criminal intent (although potentially a certain level

of disrespect for rules and authority). These attackers may cooperate with the system owner to help mitigate found vulnerabilities (e.g. through bug bounty or responsible disclosure programmes).

Insiders — Attackers with insider knowledge or access to a system, referred to as 'internals' or 'insiders' form this group, motivated by revenge or financial gain and will engage in e.g. sabotage, theft of intellectual property and fraud against their (ex-)employer (for example in [23][24][10][25][5]).

Hacktivists — The term 'hacktivists' [10][25][2] is based on the original terms 'cyber terrorists' and 'political activists' proposed in [23][24] and also supported by [18]. It refers to groups of attackers engaging in attacks with a political or social background, motivated by ideology, cause and potentially the search for fame.

Crackers & coders — This cluster consists of a number of different attacker types, including attacker types with labels such as 'crackers' [11][5]), but also 'virus writers' [9]) as well as 'elite hackers' and 'black hats' [17][3]. While these attacker types may vary regarding their level of technical skills and resources in terms of funding and equipment, they can generally be considered as very capable and knowledgeable individuals with a high potential for destruction. This group is also united by common motives behind their attacks: they will hack to feed their ego and for entertainment, but also to gain a certain reputation and status within their peer group.

Professional criminals — Professional criminals can be found across many categorisations, e.g. [16][23][24][10][25][2][18][5]. This group is defined by its criminal background and professionalism, motivated by the prospect of large financial gains. They are likely to be part of larger structures in the form of organised criminal gangs, giving them access to significant resources such as funding and technical skills also through employing highly skilled individuals to write customised malware for their attacks.

Government agents — Also described by the term 'nation states' [2][10] or 'foreign intelligence' [24], state-sponsored attackers form the 'government agents' cluster. These highly skilled attackers are employed by government agencies for the espionage, counterespionage and information monitoring of governments, individuals, terrorist groups and critical infrastructure providers (gas, electricity or water) as well as the financial or defence sectors [5]. Attackers in this cluster will have access to a vast amount of knowledge and funding due to their backing from government or government related institutions. Their appearance, general nature, targets and modus operandi may vary greatly.

Other attacker types — While the clusters derived from various attacker categorisations outlined in the last sections do not deviate significantly from other consolidated overviews on the matter (compare to [18]), there are other attacker types not covered in this summary. This is generally the case for attacker types which have not been introduced in more than one of categorisations reviewed. An example is the case of the 'crowdsourcer' attacker type newly proposed in [25] — it describes large scale human collaboration to obtain often confidential information, potentially using illegal means.

3 METHODOLOGY

This section presents a short overview on the employed methodology and data sources used to arrive at the proposed typology in Section 4. As no previous treatment for the case of digital banking appears to exist, this paper seeks to address the following research questions: what are the most common attacker types targeting digital banking systems? Which criteria are best used to describe these attackers types? Which attacker characteristics and behaviours are best used to inform these criteria?

3.1 Data sources

The underlying data used to inform the categorisation consists of over 200 freely available documents containing information about digital banking fraud cases and the attackers involved [1][12][8]. These data sources consist of news reports of digital banking attacks also containing information on the attackers as well as profile description of cybercriminals. The datasets used where chosen for their public availability, level of detail and specific relevance to digital banking. However, similar datasets containing information on such incidents could be added, like for example from the VERIS database or industry-specific shared data.

3.2 Taxonomy building process

In preparation for the taxonomy building process, the described dataset was analysed using grounded theory analytical steps. This method was chosen for its exploratory nature and ability to construct theory [4]. In contrast to solely relying on literature, the aim was to use the here discovered attacker characteristics to help build the classification criteria and ultimately the attacker profiles.

The initial grounded theory coding process yielded two axial codes (personal characteristics and social interactions; attack-related behaviours) and six main categories (personal characteristics, community, geography; modus operandi, targets, relationship with law enforcement) containing a large number of codes which further break down these categories. Through comparison to the criteria used to build other taxonomies (see Section 2.3) a number of these subordinate codes were selected as potentially useful for building the new taxonomy.

While all of these codes already had a number of text excerpts describing attacker characteristics and behaviour associated with them, a third round of coding (initial and subsequently structural coding) was carried out to make sure all the information in the data sample was captured in a structured way. All variations found under the conceptual phrases or codes was now collated and logically clustered together where possible. Attacker categories were regrouped, merged or separated as often as required. Categorisation and re-ordering was finished when all variations where accounted for and did not present any new clues for further categorisations or changes — for this study and its underlying dataset, theoretical saturation (defined in [4] p.345 or [6] p.194) had been reached at this point in time.

The results of this exercise are presented in the next section. In the spirit of grounded theory research, the proposed taxonomy should be treated as an initial step — notes on current limitations, viable verification efforts and potential further research can be found in Section 5.

4 RESULTS

Table 1: System challengers

Subgroups	System testers, fun/challenge seekers
Labels	White hat or ethical hackers, thrill seekers or glory hunters, young or novice hackers
Motives	Fun of hacking, bragging rights, challenge to break into system, exposing vulnerabilities (responsible disclosure)
Criminal intent	Low to moderate
Resources	Range of skills and funds, can be limited
Activities	System intrusion, penetration testing, publication of vulnerabilities
Level of danger posed	Relatively low, but varies across the group and can be seen as an entry into serious criminality for some
Type of risk posed	Often reputational risk, may however also be of financial or operational nature
Other notes or comments	Very heterogeneous group united by desire to overcome challenge posed by overcoming the system's defence.

Table 2: Supporters

Subgroups	Money mules, non-technical support functions
Labels	Non-technical support functions: mules, cash collectors, business functions such as recruitment, marketing or customer service
Motives	Financial gain, 'making ends meet'
Criminal intent	Moderate to high (in some cases unwittingly)
Resources	Limited technical skill levels and funding
Activities	Supporting a larger group or system through all stages of money laundering and other business support functions
Level of danger posed	Low on their own, but part of a group or system
Type of risk posed	Usually financial risk, although operational and reputational risk may be indirectly posed
Other notes or comments	Supporters are not technically attackers themselves, but support others to commit crimes

Table 3: Insiders

Labels	Banking employees, employees of third-party suppliers
Motives	Financial gain, retaliation
Criminal intent	Moderate to high
Resources	Range of skills and funds, enabled through insider knowledge and capabilities including elevated access rights
Activities	Usage of insider knowledge to extract money directly (or enable others), system destruction, industrial espionage
Level of danger posed	High, significant levels of damage possible
Type of risk posed	Often financial, but also significant potential for operational (IT sabotage) and potentially reputational risk

Table 4: Ideologists

Labels	Hacktivists, online activists or cyber terrorists
Motives	Cause, ideology, in rare cases also status and ego (secondary motives such as financial gains may be present)
Criminal intent	Moderate to high
Resources	Moderate to high skill levels and funding
Activities	Social or political background to attacks
Level of danger posed	High, significant levels of damage and destruction intended
Type of risk posed	Reputational risk and linked operational risk, financial risk as a secondary motive
Other notes or comments	Ideologists are usually motivated by cause and ideology, but examples of attackers being motivated by selfish reasons such as financial gain or simply to engage in petty vandalism can be found, for example for subgroups of Anonymous

Table 5: Officials

Labels	Nation states, sovereign countries, government or its agencies, military functions
Motives	Cause, ideology, cyber warfare
Criminal intent	High
Resources	Very high skill levels and funding
Activities	Espionage, counterespionage, information monitoring and destructive attacks, cyber warfare
Level of danger posed	High, although limited evidence and confirmed cases to date
Type of risk posed	Operational risk as a main focus with reputational and financial risk directly linked
Other notes or comments	Not much is known about this group and references in the data sample are sparse — these attacker types like to remain undetected.

Table 6: Professionals I: groups and gangs

Labels	Sophisticated large criminal groups or gangs and organised online crime syndicates, also termed as cyber mafia (members often professionally recruited)
Motives	Financial gain
Criminal intent	High
Resources	High skill levels and funding: broad range of skills and resources available through group setup
Activities	Phishing, ransomware, trojans and malware attacks as well as system intrusion at large scale, physical attacks e.g. against cash machines also possible. May also offer their services through criminal-to-criminal franchise models.
Level of danger posed	High, significant levels of damage
Type of risk posed	Financial, operational and reputational risk directly linked
Other notes or comments	Primary/key category for digital banking attackers. These attackers should be viewed as highly professional criminals.

Table 7: Professionals II: Small Groups and Individuals

Labels	Lone hackers and individual attackers, small criminal groups and gangs (can be relatives or friends rather than recruited)
Motives	Financial gain
Criminal intent	High
Resources	Moderate to high skill levels and funding
Activities	Phishing, ransomware, trojans and malware attacks as well as system intrusion at large scale, physical attacks. Similar to professionals I, but usually at smaller scale.
Level of danger posed	Medium to high
Type of risk posed	Financial, operational and reputational risk directly linked
Other notes or comments	Primary/key category for digital banking attackers. Again, these attackers should be viewed as professional criminals, and not underestimated.

Table 8: Toolkit users

Labels	Users of attack toolkits (also called crime-in-a-box, exploit or crimeware kits), clients of criminal-to-criminal services (also named crimeware-as-a-service)
Motives	Financial gain, 'making ends meet'
Criminal intent	High
Resources	Limited skills and funds (relying on toolkits), although more experienced attackers may use them for convenience and scalability too
Activities	Phishing, ransomware, trojans and malware attacks through usage of toolkits and services available through criminal-to-criminal franchises.
Level of danger posed	Medium to high
Type of risk posed	Financial risk, operational and reputational risk directly linked
Other notes or comments	Primary/key category for digital banking attackers. There may be overlaps between the former categories (professionals I and II), but the emphasis for toolkit users is on their reliance on crimeware toolkits to launch attacks and commit crimes.

5 DISCUSSION AND FUTURE WORK

There are several initial insights from the presentation of the results and the included eight attacker profiles specific to digital banking. Firstly, it seems entirely possible to build a new industry or application specific attacker typology or taxonomy. Furthermore, it is indicated that real-world data, even of secondary nature, can help to build such categorisations, providing a new perspective over categorisation solely based on previous literature.

For the specific case of digital banking, a number of new and interesting categories have emerged that have not been part of previous, more generic taxonomies. The supporters category is certainly interesting as a non-technical category — while technical mitigations may not strictly be required, banks may for example want to consider how they can deter individuals from becoming money mules or other crime supporters. The professional criminals category found in most previous categorisations has been further examined and split into three sub-categories in our proposal — this seems adequate as digital banking services could be assumed to be a particular focus of various types of professional criminals. This aspect again could help banks to re-think their perspective on human adversaries and threat agents and further tailor their defences to specific attacker groups. Lastly, the presence of attackers not driven by profit (e.g. ideologists) is also highlighted in the presented typology. Additionally, reputational risk has found inclusion into this typology — this seems particular relevant to financial institutions with their business model largely building on trust.

However, not unsimilar to previous taxonomy efforts, this initial effort leaves open several questions and challenges in this research space. Firstly, while the presented typology is grounded in real-life data, verification using further data or against similar studies has not been attempted. Similarly to previous taxonomies, the practical value and impact of the introduced typology has not been defined at this point in time. Further options for extension and integration into existing risk assessment methods and tools or threat modelling approaches have not been considered in this short paper. Lastly, due to the limited scope of this publication, several aspects have only been touched upon briefly, like the terminology or grounded theory element of this study, which should both be expanded on.

In direct relation to the last paragraph, the following future research directions are suggested at this point in time: firstly, the addition of new datasets to re-run the typology construction and tests its validity and robustness. Relating back and further comparing the new typology to previous research in this area may help to learn more about the research field in general and to produce further guidance on typology/taxonomy construction methods. Expansion on certain aspects also seems worthwhile, including research on integration points for such categorisations. This could also be helped by working with practitioners and gaining insights into their view on categorisations and their potential practical value.

In summary, as an initial starting point for a typology built 'from the ground up' , the results produced certainly seem encouraging. It will now be of interest to keep this typology up to date, discuss it with other researchers and practitioners and to feedback on the learnings so they can be integrated in future efforts in this field.

REFERENCES

[1] British Computer Society (BCS). 2010-2014. Cybercrime Forensics Specialist Group briefings. Compiled by Denis Edgar-Nevill (Canterbury Christ Church University), available via group distribution list. (2010-2014).

[2] Eric Chabrow. 2012. 7 Levels of hackers — applying an ancient Chinese lesson: know your enemies. Retrieved March 30, 2019 from http://www.govinfosecurity.com/blogs.php?postID=1206. (25th of February 2012).

[3] Amanda Chandler. 1996. The changing definition and image of hackers in popular discourse. *International Journal of the Sociology of Law* 24, 2 (1996), 229–251. DOI: https://doi.org/10.1006/ijsl.1996.0015

[4] Kathy Charmaz. 2014. *Constructing Grounded Theory* (2nd ed.). SAGE.

[5] Raoul Chiesa, Stefania Ducci, and Silvio Ciappi. 2008. *Profiling Hackers — The Science of Criminal Profiling as Applied to the World of Hacking.* Auerbach Publications.

[6] John W. Creswell. 2013. *Research Design (International Student Edition): Qualitative, Quantitative, and Mixed Methods Approaches.* SAGE.

[7] M. de Bruijne, M. van Eeten, C. H. Ganan, and W. Pieters. 2018. Towards a new cyber threat actor typology — a hybrid method for the NCSC cyber security assessment. TU Delft. (2018).

[8] Federal Bureau of Investigation (FBI). 2018. Cyber's most wanted. Retrieved March 30, 2019 from https://www.fbi.gov/wanted/cyber. (2018).

[9] Sarah Gordon. 1996. The generic virus writer I+II. *6th International Virus Bulletin Conference, Brighton, UK* (September 1996). Last retrieved from March 30, 2019 from https://www.virusbulletin.com/virusbulletin/2015/06/throwback-thursday-virus-writers-part-1-may-1999.

[10] Sara L.N. Hald and Jens M. Pedersen. 2012. An updated taxonomy for characterising hackers according to their threat properties. In *14th International Conference on Advanced Communication Technology (ICACT).* 81–86.

[11] Richard C. Hollinger. 1988. Computer hackers follow a Guttman-like progression. *Phrack Inc.* 2, 22 (April 1988). Retrieved 30th March, 2019 from http://phrack.org/issues/22/7.html.

[12] Alice Hutchings. 2018. Cambridge Computer Crime Database. Retrieved March 30, 2019 from https://www.cl.cam.ac.uk/{~}ah793/cccd.html. (2018).

[13] Intel. 2007. Threat Agent Library helps identify information security risks (information technology white paper). Retrieved March 30, 2019 from https://www.sbs.ox.ac.uk. (2007).

[14] D. J. Ivoce. 1997. Collaring the cybercrook: An investigator's view. *IEEE Spectrum* 34, 6 (June 1997), 31–36. DOI: https://doi.org/10.1109/6.591662

[15] Max Kilger, Ofir Arkin, and Jeff Sutzman. 2004. *Know Your Enemy — Learning About Security Threats.* Addison-Wesley. 503–556 pages.

[16] William Landreth. 1989. *Out of the Inner Circle: A Hacker's Guide to Computer Security.* Microsoft Press.

[17] Larisa April Long and Egan Hadsell. 2012. Profiling hackers. Retrieved March 30, 2019 from http://www.sans.org/reading_room/whitepapers/hackers/profiling-hackers_33864. (January 2012).

[18] C. Meyers, S. Powers, and D. Faissol. 2009. *Taxonomies of Cyber Adversaries and Attacks: A Survey of Incidents and Approaches.* Technical Report. U.S. Department of Energy, Lawrence Livermore National Laboratory.

[19] Nick Nykodym, Robert Taylor, and Julia Vilela. 2005. Criminal profiling and insider cyber crime. *Digital Investigation* 2, 4 (2005), 261–267. DOI: https://doi.org/10.1016/j.diin.2005.11.004

[20] Tom Parker, Eric Shaw, Ed Stroz, Matthew G. Devost, and Marcus H. Sachs. 2004. *Cyber Adversary Characterisation — Auditing the Hacker Mind.* Syngress, Rockland, MA.

[21] C. P. Pfleeger and S. L. Pfleeger. 2006. *Security in Computing.* Prentice Hall.

[22] R. Borges Da Silva. 2013. Taxonomy and typology: are they really synonymous? *Sante Publique* 25, 5 (2013), 633–637.

[23] Marcus K. Rogers. 1999. A new hacker taxonomy. Retrieved March 30, 2019 from homes.cerias.purdue.edu/~mkr/hacker.doc. (1999).

[24] Marcus K. Rogers. 2006. A two-dimensional circumplex approach to the development of a hacker taxonomy. *Digital Investigation* 3, 2 (2006), 97–102. DOI: https://doi.org/10.1016/j.diin.2006.03.001

[25] Ryan Seebruck. 2015. A typology of hackers: Classifying cyber malfeasance using a weighted arc circumplex modec. *Digital Investigation* 14 (2015), 36–45. DOI: https://doi.org/10.1016/j.diin.2015.07.002

[26] Zhengchuan Xu, Qing Hu, and Chenghong Zhang. 2013. Why computer talents become computer hackers. *Communications of the ACM* 56, 4 (April 2013), 64–74. DOI: https://doi.org/10.1145/2436256.2436272

[27] Wolfgang Ziegler and Christian S. Fötinger. 2004. Understanding a hacker's mind — a psychological insight into the hijacking of identities. Retrieved April 10, 2013 from http://www.donau-uni.ac.at/de/department/gpa/informatik/DanubeUniversityHackersStudy.pdf. (2004).