CHARLES UNIVERSITY

FACULTY OF SOCIAL SCIENCES

Institute of Political Studies

Department of Political Science

Master's Thesis

2022 **Anna Valentová**

CHARLES UNIVERSITY

FACULTY OF SOCIAL SCIENCES

Institute of Political Studies

Department of Political Science

Testing the applicability of hacker typologies and models: A comparative case study of Fancy Bear and The Shadow Brokers

Master's thesis

Author: Anna Valentová

Study programme: Security Studies

Supervisor: prof. PhDr. RNDr. Nikola Hynek, Ph.D., M.A.

Year of the defence: 2022

Declaration

1. I hereby declare that I have compiled this thesis using the listed literature and resources only.
2. I hereby declare that my thesis has not been used to gain any other academic title.
3. I fully agree to my work being used for study and scientific purposes.

In Prague on Monday July 18, 2022 Anna Valentová

References

VALENTOVÁ, Anna. *Testing the applicability of hacker typologies and models: A comparative case study of Fancy Bear and The Shadow Brokers*. Praha, 2022. 67 pages. Master's thesis (Mgr.). Charles University, Faculty of Social Sciences, Institute of Political Studies. Department of Security Studies. Supervisor prof. PhDr. RNDr. Nikola Hynek, Ph.D., M.A.

Length of the thesis: 109 878 characters with spaces from Introduction to Conclusion.

Abstract

The Master's Thesis named "Testing the applicability of hacker typologies and models: A comparative case study of Fancy Bear and The Shadow Brokers" focuses on different categorization techniques of hacker groups. It explains how hackers are studied in the field of social sciences and theoretical and practical cyber security. The thesis aims to test the disciplines and applicability of their typologies and models on two cases – The Shadow Brokers and Fancy Bear, hacker groups representing a novel type of threat actor. Firstly, the theoretical section focuses on explaining typologies and models while also representing the trends and evolution of research on hackers. Secondly, a practical part of the thesis picks a few frameworks to be tested via the two cases. After the testing, the virtues and shortcomings of the frameworks are analysed, and the approaches of disciplines are compared. The practical part of the thesis shows there is no unified approach to studying hacker groups and almost all previous ones are not applicable to the two hacker groups cases. Therefore, based on the results, the dimensions for a new typology are proposed with the objective of creating a stepping stone for an applicable approach to studying hacker groups in security studies research.

Abstrakt

Diplomová práce s názvem „Komparativní analýza hackerských skupin The Shadow Brokers a Fancy Bear: testování aplikovatelnosti typologií a modelů" se zaměřuje na techniky kategorizování hackerských skupin. Vysvětluje, jak se hackeři studují v oblasti společenských věd a teoretické i praktické kybernetické bezpečnosti. Práce si klade za cíl otestovat disciplíny a použitelnost typologií a modelů na dvou případech – The Shadow Brokers a Fancy Bear, hackerských skupin představujících novodobý typ aktéra. Teoretická část se zaměřuje na vysvětlení typologií a modelů a zároveň představuje trendy a vývoj výzkumu hackerů. Praktická část práce poté vybírá několik rámců, které budou testovány prostřednictvím těchto dvou případů. Po testování jsou analyzovány přednosti a nedostatky různých typologií a modelů a porovnávány přístupy oborů k výzkumu. Praktická část práce dokazuje, že neexistuje jednotný přístup ke studiu hackerských skupin a téměř všechny předchozí rámce nejsou aplikovatelné na dva testované případy. Na základě výsledků jsou proto navrženy dimenze pro novou typologii, které si kladou za cíl vytvořit odrazový můstek pro nový přístup ke studiu hackerských skupin v oblasti bezpečnostních studií.

Keywords

Hacker Typologies, Hacker Categorization, Cyber Threat Actor Profiling, Fancy Bear, The Shadow Brokers;

Klíčová slova

Typologie hackerů, Kategorizace hackerů, Profilování aktérů kybernetických hrozeb, Fancy Bear, The Shadow Brokers;

Title

Testing the applicability of hacker typologies and models: A comparative case study of Fancy Bear and The Shadow Brokers

Název práce

Komparativní analýza hackerských skupin The Shadow Brokers a Fancy Bear: testování aplikovatelnosti typologií a modelů

Acknowledgement

I would like to express my gratitude to my supervisor prof. PhDr. RNDr. Nikola Hynek, Ph.D., M.A. for his comments and guidance that were highly appreciated.

Table of Contents

Introduction

In today's world, technology dominates most of our lives. The speed of its development corresponds with its implementation into the daily routine of any average person. With the advantages that technology brings us, however, also come novel issues and threats that the experts must deal with. Due to the diversification of the population on the Internet, a wider and more diverse spectrum of cyber activity appears every day. Amongst the users who use the Internet for sharing and getting information without any bad intentions, are actors who consciously take an advantage of the loopholes in security systems, who find ways to break through cyber walls which were made to protect data and who harm institutions, governments, organizations, and other users. The Internet has changed and grown so much since it was established, that it comes as no surprise that a term used to describe this type of actor also changed its meaning.

It was already in the 1970s when the word "hacker" was used as a tech term.[1] Back in those times, a hacker was an enthusiast with advanced computer technology skills. Since then, not only the meaning of the word has changed, but also its essence. Even the people not interested in technology have probably heard of the term "hacker group". Maybe in relation to Russian hacker groups allegedly attacking the United States, Stuxnet, the 2007 attacks on Estonia, and the attack on Sony Pictures, or maybe they have at least heard the name of some infamous group, such as Anonymous, Fancy Bear or many others.

Even though the cyber experts dealing with these groups found ways to reveal the nature of the hackers, the actions on the Internet are now complex and complicated more than ever. Even if we manage to pinpoint the nationality of the attackers, there always is an issue with the attribution of the attack. Many IT experts are able to find pieces of the identity of the hackers through code and other measures, however, based on the existing literature, I believe, the field of cyber security needs to be studied to greater lengths from the perspective of security studies. The issue is also not only with the identity, and attribution, but with the motivation, lessons learned from the event, and other factors as well. Since the emergence of the word "hacker", the researchers have devoted their time to studying the phenomena and strived to create typologies with specific categories, that did

[1] Gevirtz Morris. (2019, February 22). *The History of the Word "Hacker".* Deepgram. https://deepgram.com/blog/the-history-of-the-word-hacker-2/.

not only help to study the hackers in theory, but in time also started benefiting the field of cyber security, and experts from this field began utilizing and updating the existing categorization techniques for their own research purposes and for cyber security in practice.

So far, however, no study of this depth that tests the approaches from different disciplines has been conducted. Therefore, together with carefully picked cases, I strive to contribute to this phenomenon by comparing some of the categorization techniques that are used by social scientists, cyber experts and works meant to be applicable in practice. Researching the three disciplines in one study would help to achieve the goal of this thesis, which is to conduct multi-disciplinary comparative research of typologies and models with the objective of elevating the field of study, helping it to be accordingly complex to the state of cyber affairs, and finally if possible, proposing an approach to study the hacker groups or threat actors based on the results of cases testing.

Research target, research question

The goal of this thesis is to test the existing frameworks of studying hacker groups from the disciplines of social sciences, cyber security, and cyber security/IT practice, and evaluate their approaches. The thesis also aims at comparing the results of the tests by detecting issues, virtues, and possible similarities of tested typologies and models. The hacker groups subjected to testing were chosen since they both represent a novel type of threat actor, which helps to test the applicability of the older as well as newer frameworks. Furthermore, each of the groups also represents a different type of hacker with very little data in one case and a bigger amount of information in the other, helping to study the categorization techniques with one actor hypothetically passing the tests easily due to a larger number of data, and other with more difficulties due to the lack of data. This concept could also uncover if the typologies can produce the same results even if approached with a problem case. After subjecting the typologies and models to examination, the second goal of this thesis is to propose a new typology based on the results of all disciplines' testing. The results are utilized to evaluate the importance of each factor used to categorize a certain type of hacker and propose a newly updated typology of threat actors, hereby contributing to the research of all three disciplines.

The research questions are therefore as follows: What are the issues and virtues of tested typologies and models? What similarities do they share? Are these frameworks also applicable to the novel types of threat actors? Which dimensions and factors have proven to be important after testing? What would the proposed updated dimensions in threat actor typology look like?

Empirical data and analytical technique

This thesis will be conceived as a conceptually driven comparative analysis. By using two cases of modern hacker groups Fancy Bear and The Shadow Brokers, it will test the existing concepts outlined below and try to adapt them to create a new conceptual framework to study the hacker groups in security studies. My motivations behind picking these two groups are first, that they emerged recently, and both have very interesting modus operandi or alleged connection to the Russian state. This is important for my thesis because it encompasses both ideological motivations and other attributes that could be typical for other novel threat actors, while at the same time being sufficiently different to provide greater evidential value to the testing. The sophistication of the groups played another crucial factor. I hope that by picking a sophisticated actor, the contribution of my analysis to security studies would be of greater benefit.

The hacker groups are subjected to testing of different typologies and models that are chosen from examining a conceptual and theoretical framework that also stands for a literature review in this thesis since it encompasses the most important literature for the research. Based on the chosen typologies and models, I am deriving the factors by which the study is conducted in the second part, the analytical part of testing. The empirical data for this part are going to be collected from secondary sources, and case studies of different hacker groups on the topic of their modus operandi. Furthermore, since I am a social scientist and am not able to decode the technical data by myself, I collect data from cyber security experts' studies, who have researched both The Shadow Brokers and Fancy Bear, and use this data to conduct the tests of previously chosen concepts from different disciplines. In this part I focus on the criteria the researchers have chosen to be valuable for their typology and research the hacker groups based on their concepts.

This information will be gathered via different attacks and possibly other online activities, such as social media, of the groups, which should find overlapping issues, virtues, and similarities of the tested concepts. I plan to find out the best typology and model, and finally, based on the results of the testing, I try to propose a typology that could correspond with the state of cyber adversaries.

My thesis is therefore a comparative multi-disciplinary process-based analysis, which uses two important questions popular in social sciences research for their ability to provide a complex analysis of an issue. The first question targets the modus operandi, how do the groups work. The second covers their motivations, why they do what they do. My thesis also strives to connect cyber security methods with techniques used in social sciences, intending to benefit the field of security studies.

Structure of the thesis

The first part of my thesis focuses on the conceptual framework, where the typologies and models from the field of social science and cyber security research, as well as cyber security in practice, are going to be introduced. This section explains the categorizations techniques chronologically from researchers from all three disciplines.

Secondly, I explain the chosen concepts from the first part and the specific hacker groups in greater detail. This part is followed by researching the hacker groups via previously described typologies and creating the models of the hacker groups based on the author's propositions. Thirdly, the results of the tests are discussed and insufficiencies, similarities, and qualities of different typologies as well as disciplines are debated and compared.

Finally, based on the comparisons and other findings, while also considering the specific cases, I propose a new typology, which could eliminate the issues found during testing and is suggested for further research with different cases to find out its new applicability.

1. Conceptual/theoretical framework - Introduction to the models and concepts

How are hacker groups studied?

It is important to describe how have hackers been studied in the past, so it is easier to understand the current trends in research as well as my choice of typologies, models, and taxonomies to test in this thesis. This section also serves as a literature review since it discusses the studies used in this thesis. Firstly, it describes the evolution of hacker group studies through the lens of social sciences as well as its recent interweaving with cyber security from the technical point of view. Secondly, it explains the choice of models and typologies/taxonomies to test in this thesis. To paint a whole picture of hacker studies, one taxonomy is chosen solely from the field of social sciences, one is picked from the grey area where the previous works of social scientists intersect with cyber security experts. And finally, one last framework is representing the approach of a strictly cyber security perspective describing how the typology is applied in praxis.

1.1. How hackers used to be studied within social sciences:

The meaning of the word "hacker" developed in the academic environment in the second half of the 20th century, when people, backed by the U.S. government, collaborated on shared goals but competed for recognition amongst themselves. Its positive connotation significantly changed in the 1990s with the rise of the Internet, when computer networks suddenly became perceived as property and the community tried to differentiate between the old-school harmless and beneficial hacker, also known as white-hat hackers, and the malicious black-hat hackers with criminal intents by calling them "crackers".[2] Nevertheless, this name did not stick since the media tended to use the word "hacker" for describing all criminal activity relating to technology.[3] This term has also been widely used by researchers who have studied hackers and hacker groups. Although the cyber security community now prefers the terms "attackers" or "threat actors", as presented in 1.2. section

[2] Wark M. (2006). Hackers. *Theory, Culture & Society*, 23(2-3), 320-322. https://journals.sagepub.com/doi/10.1177/026327640602300242.

[3] Yagofa, B. (2014). A Short History of "Hack". *The New Yorker.* https://www.newyorker.com/tech/annals-of-technology/a-short-history-of-hack.

of this thesis. However, to provide a comprehensive approach, this thesis is using the word "hacker" as an all-encompassing term.

An important book that has greatly influenced the field of social sciences, called "Hackers: Crime in the Digital Sublime", was written in 1999 by Paul A. Taylor. His work encompasses the trends in academic research of hackers during the second half of the 20th century. Taylor focuses on the evolution of the meaning of the word "hacker", and on the history of hacking culture, where he explains ethics and the community. The second chapter covers motivation and follows academic theories that aim at explaining why hackers hack.[4]

However, the first attempts at the categorization of hackers can be dated already back to 1976 when Weizenbaum recognized a type he called a compulsive programmer/hacker. The type described a person, who is obsessed with technology and addicted to programming.[5] It is important to note though, that in the seventies the word "hacker" had a completely different meaning. Simply put, it did not have the same negative security risk connotations that it has today.[6] Although many academics agreed with the notion of the hacker as an addicted person escaping reality, even then this description dealt with criticism.[7]

Another early attempt to classify hackers happened in 1985. Landreth diversified five types of hackers based on motivation, which included mischief, intellectual challenge, thrill, ego boost, criminal profit, and their skills, creating five categories (*novices, students, tourists, crashers, thieves*).[8] More scholars proposed other classifications as well. For example, in 1988, Holliger recognized types only based on their skills creating three

[4] Taylor, Paul A. (1999). *Hackers*. Taylor & Francis Ltd / Books. https://search.ebscohost.com/login.aspx?direct=true&db=sih&AN=18059913&lang=cs&site=ehost-live.

[5] Taylor, Paul A. (1999). "Chapter 3: The Motivations of Hackers." In *Hackers*, 45–66. Taylor & Francis Ltd / Books. https://search.ebscohost.com/login.aspx?direct=true&db=sih&AN=18059913&lang=cs&site=ehost-live.

[6] Hannemyr, G. (1997). *Hacking considered constructive*. Oksnoen Symposium on Pleasure and Technology. http://home.sn.no/home/gisle/ oks97.html.

[7] Taylor. (1999). "Chapter 3: The Motivations of Hackers." In *Hackers*, 45–66.

[8] Landreth, B. (1985). *Out of the inner circle: a hacker's guide to computer security*. Microsoft Press.

categories of *pirates, browsers*, and *crackers*. Whereas in 1996, Chantler proposed categories based on the hackers' knowledge, motivation, prowess, and length of time involved, presenting three types of hackers: *losers and lamers, neophytes, and elites*.[9]

In general, motivation is a strong, reoccurring theme in the study of hackers in social sciences. Taylor himself also proposed six categories of hackers' motivations including the already mentioned *Feelings of addiction,* where hacking was regarded as an obsessive urge that vastly worried the parents of young hackers. *The urge of curiosity,* a less extreme and more positive motivation, in which curiosity is the driver behind technological development. *Boredom with educational system,* which happened when hackers did not find the formal learning environment sufficiently challenging, therefore they decided to educate themselves in computing alone. *Enjoyment of feelings of power*, which was described by the hackers for example as a feeling one has while in secrecy with close friends running an informal network of 250 computers. *Peer recognition,* when even though most hackers were seen as loners avoiding social interaction, in reality, they were a part of a wide hacker community, where they socialized with other hackers and strived at being recognized as a skilful and knowledgeable member of this community. And finally, *Political acts,* a motivation where hackers saw themselves as a principal force that opposes traditional values, such as physical property rights, in the newly emerging information society. Taylor also recognized a possibility of fluidity between these areas.[10]

However, the author did not focus only on categorization, he also discussed the security weaknesses that allow hackers to penetrate computer systems and the reasons behind their existence. According to Taylor, the computer security flaws were embedded in both the technical and commercial state of the industry. He argued that there was a tendency to skimp on security measures and that both the academic and business sectors are adversely affected by insufficient education about computer security. The cooperation between the computer security industry and hackers was supposedly negatively affected by social rather than technical reasons. Furthermore, he preached, that there was a problem with under-reporting hacking incidents since many times a breach happened unnoticed, or

[9] Meyers, C., Powers, S., Fassiol D. (2009). Taxonomies of Cyber Adversaries and Attacks: A Survey of Incidents and Approaches. *Lawrence Livermore National Laboratory*. https://www.osti.gov/biblio/967712/.

[10] Taylor. 1999. "Chapter 3: The Motivations of Hackers." In *Hackers*, 45–66.

companies were willingly quiet due to public embarrassment or loss of investor or public confidence concerns.[11]

1.2. How the studies have changed

Since Taylor's work the internet as well as hackers changed significantly. As Seebruck noted in his article written in 2015, the researchers tend to deviate from using typologies, in which the dimensions depict concepts or ideal types without including empirical cases and are based on qualitative data.[12] Contrary, some scholars are drawn more to the use of taxonomies, which tend to be associated usually with biological sciences. However, regardless of the name, a consensus exists on the need to classify hacker groups.[13] Therefore, the terms taxonomies and typologies are going to be used interchangeably in this thesis.

According to Seebruck, classifying has its use also outside of research. The administrators of critical infrastructures such as computer networks can also benefit from this phenomenon.[14] In the area of critical infrastructure preparedness is a vital component of crisis management. However, being prepared for all threats is deemed impossible, therefore risk management, specifically the act of reducing the number of threats by discarding the low-priority ones, is the solution to this problem.[15] Since the administrators strive for cost-effective threat mitigation, not elimination, the categorization of threats is one of the available risk management strategies. The classification system allows for the creation of an attacker's profile, creates a better understanding of which cyber security strategies are the most suitable, and helps the organizations to understand how much money they should invest in them. Furthermore, it also makes the work with statistics that

[11] Taylor. (1999). "Chapter 4: State of the Industry." In *Hackers*, 67–91.

[12] Seebruck, R. (2015). A typology of hackers: Classifying cyber malfeasance using a weighted arc circumplex model. *Digital Investigation,* 14, 36-45. https://www.sciencedirect.com/science/article/abs/pii/S1742287615000833

[13] Seebruck. (2015). A typology of hackers: Classifying cyber malfeasance using a weighted arc circumplex model.

[14] Ibid.

[15] Arjen, B., McConnell, A. (2007). Preparing for critical infrastructure breakdowns: the limits of crisis management and the need for resilience. *J Conting Crisis Manag, 15*(1), 50-59. https://onlinelibrary.wiley.com/doi/10.1111/j.1468-5973.2007.00504.x

can be utilized in cyber security easier as well as it helps the organizations to stay on top of newly emerging threats.[16]

1.2.1. Rogers's two-dimensional circumplex approach (2006)

A greatly important work in the field of social sciences was created in 2006 by Marcus K. Rogers. He revised his previous taxonomy framework concerning the one-dimensional approach and expanded it to a two-dimensional classification model more suitable for model testing.[17] Rogers and many other authors (Rogers and Ogloff, 2004; Skinner and Fream, 1997; Taylor and Loper, 2003) stress the idea that not only technical controls in the IT realm are needed to deal with hacker groups. Equally as important is the ability to understand the individuals behind the attacks.[18]

Rogers's two-dimensional circumplex approach classifies the hackers according to their skills as well as their motivation. He builds on the model he created in 1999, which was updated by Furnell in 2002 and the work of Sarah Gordon in 2001. Rogers's taxonomy includes nine primary categories starting at the level with the lowest technical skills and ending with Information Warriors as the most capable category. He also includes Political Activists as a proposed category but excludes it from his research since according to his opinion, the true motivation for their activity is too speculative to be included.[19]

It is important to include the description of the nine categories since it is vital for understanding the circumplex model, and for the way the research has developed. Therefore, the categories are as follows:

1. *Novice (NV)*

[16] Seebruck. (2015). A typology of hackers: Classifying cyber malfeasance using a weighted arc circumplex model.

[17] Rogers, M. K.. (2006). A two-dimensional circumplex approach to the development of a hacker taxonomy. *Digital Investigation 3,* 97–102. https://reader.elsevier.com/reader/sd/pii/S1742287606000260?token=68D1DEE0D78E4F90219BF4B7AE691EBF9B368EF88ACF87E35E4ED98C9622CA1C042025C44FCA26E7A065719E6C38D094&originRegion=eu-west-1&originCreation=20220326154410.

[18] Rogers. (2006). A two-dimensional circumplex approach to the development of a hacker taxonomy.

[19] Rogers. (2006). A two-dimensional circumplex approach to the development of a hacker taxonomy.

The least skilled category where hackers rely only on toolkits, the pre-written pieces of software available on the internet. Most individuals in this category are supposed to be young and show signs of deviant computer behaviours with their primary motivation being seeking thrill and ego satisfaction.[20] Rogers links this type of behaviour to the one found in youth gangs, specifically to the rule that demands the new members to commit a crime to be fully accepted into their group. The author also states that this need of proving themselves combined with low technical skill and knowledge is not to be taken lightly, since it is a very dangerous combination.[21]

2. *Cyber-punks (CP)*

The second category consists of people who can write code, even if simple and have a better understanding of computer technologies. Rogers argues they are oriented at various malicious activities such as defacing web pages, spamming via emails, credit card number theft (including identity theft), and telecommunications fraud. Their primary motivations include seeking media attention, for which reason they usually target high-profile victims, and in some cases also monetary gain.[22]

3. *Internals (IN)*

Rogers finds this category as the most dangerous one since the attacks of Internals are the costliest ones and have the biggest impact. These hackers are resentful employees/ex-employees such as IT professionals and administrators, who utilize their access privileges to attack their own organization's systems. Their skills are logically relatively good and their motivation springs from feelings of being wronged or overlooked so much that they seek revenge.[23]

4. *Petty Thieves (PT)*

[20] Furnell, S. (2003). *Cybercrime: Vandalizing the Information Society*. Addison-Wesley. https://link.springer.com/content/pdf/10.1007%2F3-540-45068-8_2.pdf.

[21] Rogers. (2006). A two-dimensional circumplex approach to the development of a hacker taxonomy.

[22] Ibid.

[23] Ibid.

The fourth category is criminals that seek to enhance their abilities by hacking. This type of hacker tends to stay in secret because of the nature of its job. They also choose to redirect their criminal activities online since it is a new realm for their traditional targets. Petty Thieves can be very skilful, and their motivation is mostly financial gain and in some cases revenge.[24]

5. *Virus Writers (VW)*

This group of hackers tends to be a sub-category of others as well as a lone-standing one. Rogers states that it is difficult to fit it into his taxonomy. Even though he claims that more research needs to be conducted on this category, the common factor of these hackers is that they age out of their deviant behaviour once they hit their middle to late twenties.[25]

6. *Old Guard hackers (OG)*

What creates this category is supposed disrespect for personal property and usual no criminal intent. These people see themselves as first-generation hackers following their ideology as well. The OG are very skilled and tend to write code and scripts for others to use but not use them themselves. Their motivation is supposed to be curiosity and intellectual challenge.[26]

7. *Professional Criminals (PC)*

The motivation of Professional Criminals is not surprisingly financial gain. They are supposed to be highly skilled, and more mature both chronologically and psychologically. In most cases, the PC are able to avoid detection by authorities and the media. The individuals from this group can be “employed” by organized criminal groups.[27]

8. *Information Warriors (IW)*

Rogers claims this category “comprises those individuals whose job is to conduct or defend against attacks designed to destabilize, disrupt, or affect the integrity of data or

[24] Ibid.

[25] Ibid.

[26] Ibid.

[27] Ibid.

information systems that command and control decisions are based upon."[28] State-sponsored groups for technology-based warfare are usually included in this category. For obvious reasons, these hackers are well trained and extremely skilled, and their motivation is patriotism. Together with Professional Criminals, they are the most dangerous hacker groups as well as the least studied since the nature of their work, methods, and attacks stay mostly secret.[29]

9. Political Activist (PA)

Rogers proposes this as the last category, however, he states that at the time he was creating this typology, the motivation of PA and speculations about their activities were not yet known enough to discuss them in detail.

The circumplex model

Rogers uses all these nine categories to update his research model. Since the variables of motivation and skills are interrelated, therefore there is a complex relationship between them, Rogers proposes a circumplex model. The position of variables on the circumference and the radius is important in this type of model since related variables are traditionally depicted nearer to each other, negatively correlated variables opposite each other, and unrelated variables are orthogonal. Rogers, however, updates the traditional concept of variable positioning by introducing modified quadrant ordering criteria. Specifically, opposite, orthogonal, and same quadrant, where the position inside the quadrant replaces the location on the circumference. The second modification concerns the skill level, which is depicted by the location of the variable relative to the origin. Meaning the further the variable is from the centre of the radius, the higher the skill level of the hackers as seen in Figure 1.[30]

[28] Ibid.

[29] Ibid.

[30] Ibid.

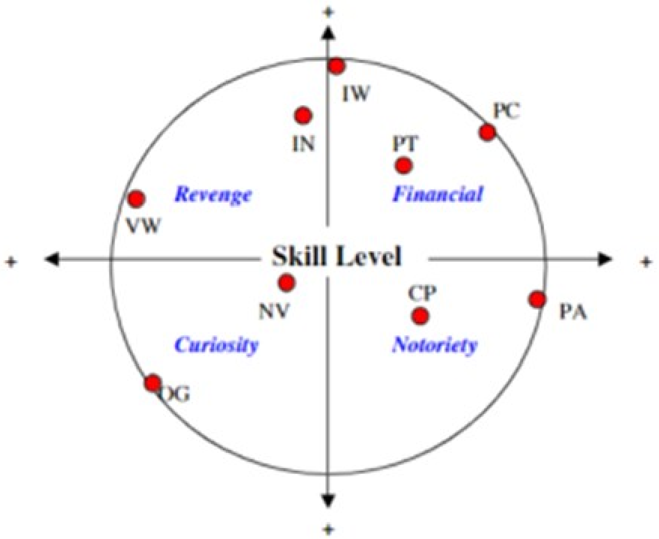


Fig. 1 – Roger's circumplex. Note: Novice (NV), Cyber-punks (CP), Petty Thieves (PT), Virus writers (VW), Old Guard hackers (OG), Professional Criminals (PC), Information Warriors (IW), Political Activists (PA), PA is included as a discussion point only.

[31]

The four quadrants for describing motivation are represented by four categories: curiosity, notoriety, revenge, and financial. Where curiosity encompasses the desire for knowledge, thrill-seeking, and other intellectual motivations. Notoriety includes media attention, gloating, and seeking fame and recognition as a folk hero character. Revenge is driven by a personal and institutional grudge or targeted against nation-states. Under the financial category falls the motivation such as greed, and personal financial gain. However, Rogers also acknowledges that these categories for the hackers' motivations are probably not sufficient enough but serve as a good base for further research.[32]

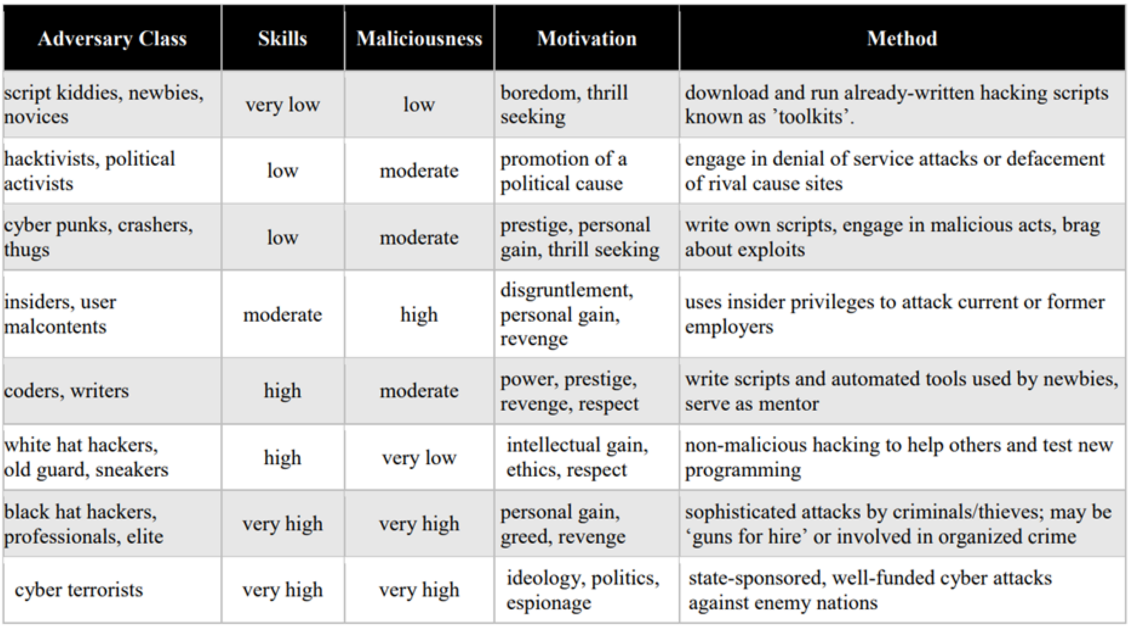
The author states that his model is not only useful as a research development tool, but it could also serve as an investigative tool. He proposes using this model in a psychological crime scene analysis, where the perpetrator leaves behind leads that are called the salient case points (SCP) and include information about the victim, artefacts left such as running programs, uploaded scripts or messages, and type of compromised data, degree of forensic knowledge (what the attacker did to hide his tracks), and level of violence. Using the knowledge with the model could help the investigators to include the

[31] Ibid.

[32] Ibid.

perpetrator into a category which could reduce the number of possible suspects and speed up the process.[33]

1.2.2. Meyers et al. updated taxonomy (2009)



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 1. Meyers et al.'s Taxonomy [34]

Meyers et al.'s work is also particularly important since future researchers are basing their updated models on it.[35] The researchers have expanded the factors by which the hackers are studied from only skill level and motivation to maliciousness and method as well. The table below represents Meyers et al.'s new taxonomy. They have also included a new category called "cyber terrorists" instead of *Information Warriors* and *Political Activists* Rogers had created. They argued this group is the most dangerous and skilled. As examples, the researchers included the attack on Estonia in 2007 after the

[33] Ibid.

[34] Meyers et al. (2009). Taxonomies of Cyber Adversaries and Attacks: A Survey of Incidents and Approaches.

[35] Seebruck. (2015). A typology of hackers: Classifying cyber malfeasance using a weighted arc circumplex model.

removal of a Russian World War II monument and the wave of DDoS attacks on Georgia in 2008.[36]

Even though Meyers et al. also created a taxonomy for cyber attacks, their updated circumplex model does not include method or maliciousness. It depicts motivation and skills in the same manner as Rogers's work.[37]

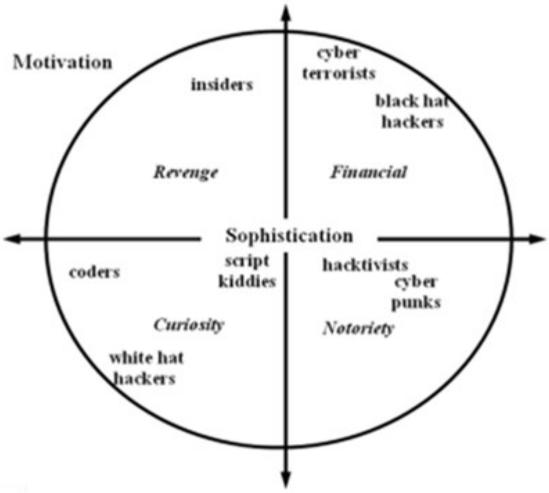


Fig. 2 - Meyers et al.'s circumplex model

[38]

1.2.3. Hald and Pedersen's Update (2012)

Hald and Pedersen did another update of Rogers and Meyers's taxonomies. They proposed mostly a new terminology and updated the categorization based on the terms widely used in the security and criminal law community. Specifically, they interchanged the *Novice* category with the term "Script Kiddies", combined the problematic group *Virus Writers* with *Cyber-Punks* and placed their motivation towards notoriety seeking. Based on the security community renamed *Internals* to "Insiders" and the *Old Guard Hackers* to "Grey Hat", dissolved the *Information Warriors* category to the *Professional Criminals* for the hackers with financial motivation, and created a new one called "Nation States" for the remaining part motivated by their ideological beliefs. Finally, they revised the name Political Activists to the newly commonly accepted term "Hacktivists". The researchers

[36] Meyers et al. (2009). Taxonomies of Cyber Adversaries and Attacks: A Survey of Incidents and Approaches.

[37] Ibid.

[38] Ibid.

have also included threat properties for each category, describing the Type, Intent, Triggers, Capability – Skills, Capability – Resources, Methods, and Trends and they created tables with these dimensions for each type of hacker. Nevertheless, their circumplex model depicts the categories of hackers in the same manner as the previous ones, only the position of the categories has changed based on the threat properties they encompass.[39]

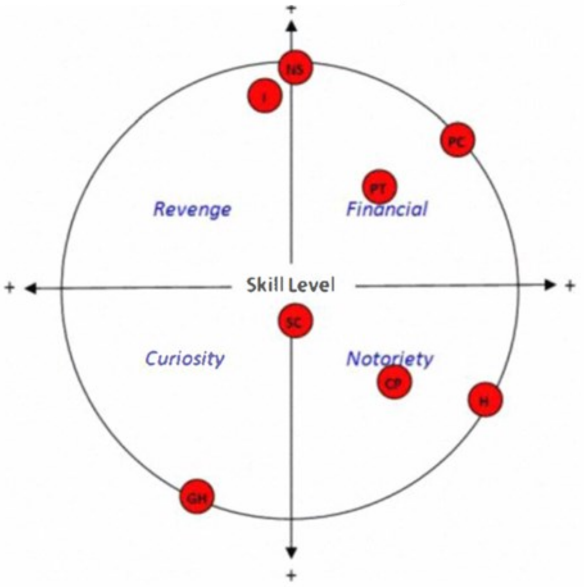


Fig. 3 - Hald and Pedersen's circumplex model [40]

1.2.4. Donalds and Osei-Bryson (2014)

In 2014, Donalds and Osei-Bryson revised the existing hacker classification due to the need for a cybercrime taxonomy. They have differentiated *Insiders* from those who are motivated by revenge and created a new category called *Corporate Raiders* for those with the same background, but financial motivation. They also added two new categories. The first one is called *Digital Pirates* or *Copyright Infringers* and encompasses the hackers that are motivated by commercial advantage, financial gain, or notoriety. On the internet, they

[39] Hald, S. LN., Pedersen, J. M. (2012). An Updated Taxonomy for Characterizing Hackers According to Their Threat Properties. In *14th International Conference on Advanced Communication Technology (ICACT)*, 81-86. *IEEE*. https://ieeexplore.ieee.org/document/6174615.

[40] Hald and Pedersen. (2012). An Updated Taxonomy for Characterizing Hackers According to Their Threat Properties.

usually duplicate, distribute, download, display or sell copyrighted digital material. The second category is called *Online Sex Offenders/Cyber Predators/Pedophiles*, whose motivation and actions are self-explanatory. The authors have also created two new motivation categories. Political/Ideological being the first one, and Sexual Impulses the second.[41]

It is also interesting that for analysing cybercrime, the hackers' taxonomy is used together with Tool & Tactic, Impact (a direct consequence of attackers‘ actions), Result (direct consequence of the impact, f.e. monetary loss, reputational damage, or no harm), Relationship (between the victim and attacker), Target, and Offence (legal label).[42]

1.2.5. Seebruck's updated circumplex model (2015)

A great contribution to the research of hackers in social sciences was done by Seebruck in 2015. He argued that the circumplex models created so far omit that in real life, hackers are not motivated only by one or two things. For that reason, he replaced the nodes representing the hacker groups in their motivation quadrants with arcs. The so-called weighted arc circumplex model is supposed to capture multiple motivations as well as their intensity, where the thickest arc indicates primary motivation and thins proportionally to secondary, tertiary, and so on.[43]

Seebruck taxonomy is built upon the foundation of Rogers and Meyers et al. He however argues that the hacktivist group is motivated by ideology rather than notoriety, therefore the cyber defence systems would benefit by updating the hacker typology on this basis. Furthermore, Seebruck stresses that the previous typologies do not include a new type of hackers that developed only recently – the socially motivated malicious crowdsourcers. This new type of hackers encompasses online movements that aim at solving a problem collectively, with possibly questionable methods or for disreputable

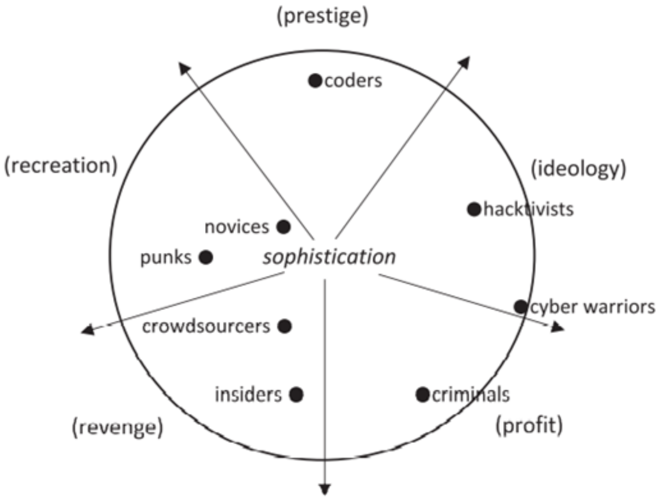
[41] Donalds, Ch. Osei-Bryson, K-M. (2014). A Cybercrime Taxonomy: Case of the Jamaican Jurisdiction. *CONF-IRM 2014 Proceesings 5.* http://aisel.aisnet.org/confirm2014/5?utm_source=aisel.aisnet.org%2Fconfirm2014%2F5&utm_medium=PDF&utm_campaign=PDFCoverPages.

[42] Donalds, Ch., Osei-Bryson, K. (2014). A Cybercrime Taxonomy: Case of the Jamaican Jurisdiction.

[43] Seebruck. (2015). A typology of hackers: Classifying cyber malfeasance using a weighted arc circumplex model.

reasons such as doxing, which in its shadiest form means hacking into social media accounts to get access to private information and publicly revealing them.[44]

On this basis, Seebruck adds a new motivation to the circumplex model – ideology and reclassifies the previous curiosity, notoriety, revenge, and financial gain to recreation, prestige, revenge, and profit. Ideology includes the types of political activists motivated by contemporary social issues nationalists, who represent patriotic civilians or state-sponsored attackers. Recreation encompasses those who hack for pleasure: intellectual, thrill, and mischief. Prestige is defined by hackers who do not seek monetary gain, are not malicious and hack for notoriety (f.e. white hackers). Profit is the motivation of money seekers and Revenge includes personal vengeance as well as larger social justice issues (f.e. crowdsourcers). Seebruck's hacker types then include *novices, crowdsourcers, punks, hacktivists, insiders, criminals, coders, and cyber warriors*. A typical circular order circumplex model according to Seebruck is depicted in Fig. 4.[45]



Notes: Nodes depict hacker types; nodes placed nearer to circle edges are more sophisticated; regular text indicates hacker groups; parenthesized text indicates motivations.

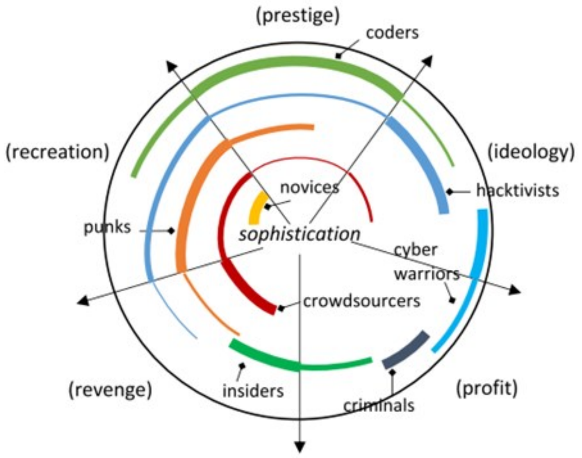
Fig. 4 - Seebruck's circular order circumplex model [46]

Seebruck's weighted arc circumplex of hacker types is then represented by Fig. 5:

[44] Ibid.

[45] Ibid.

[46] Ibid.



Notes: Thick arc segments indicate primary motivations; correspondingly thinner arc segments indicate secondary, tertiary, or quaternary motivations; notes from Figure 1 still apply.

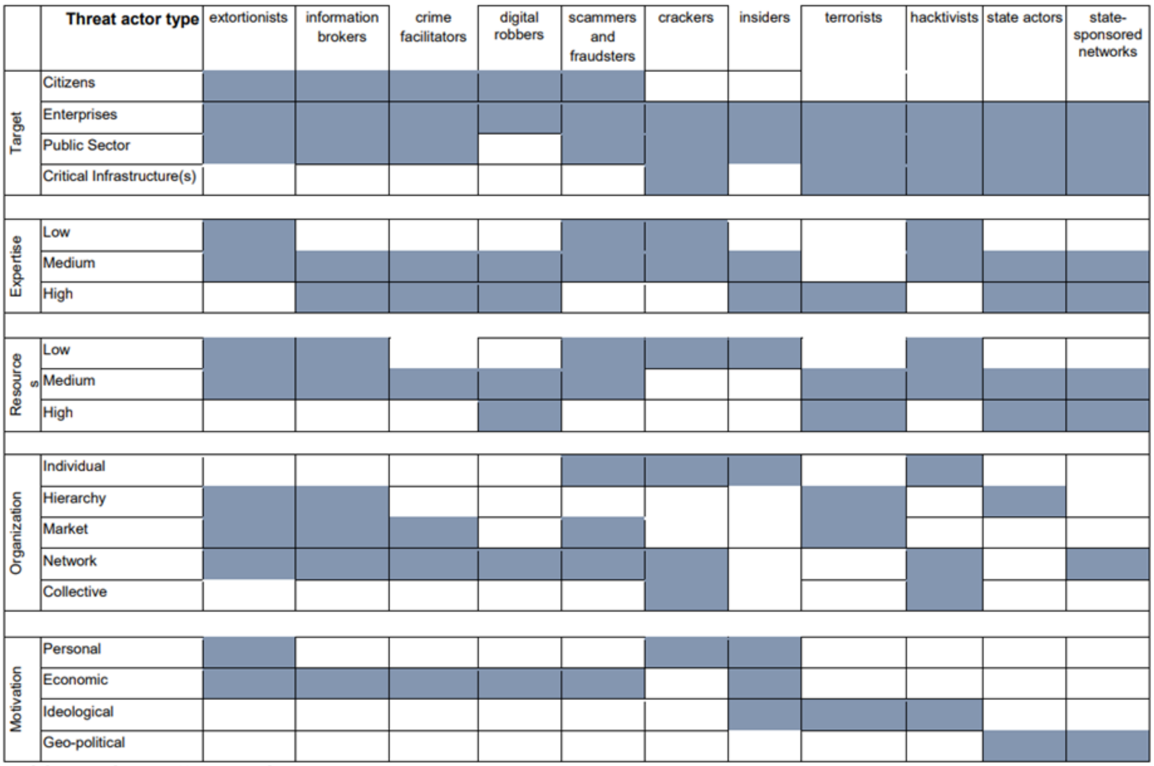
Fig. 5 - Seebruck's weighted arc circumplex model [47]

[47] Ibid.

1.3. Recent way of studying hacker groups: when social science meets cyber professionals

In the last 5 years, more approaches have been drawn up and previous models updated. Specifically, the categorizations of hacker groups that were created by social scientists were updated by cyber security professionals. It is important to describe these updates since they represent the usefulness of social science in other fields of research.

1.3.1. de Bruijne et al. (2017)



	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		■	■	■			■	■		■	■
Resource s	Low	■	■			■	■	■		■		
	Medium	■	■	■	■	■			■	■	■	■
	High				■				■		■	■
Organization	Individual					■	■	■		■		
	Hierarchy	■	■						■		■	
	Market	■	■	■		■			■			
	Network	■	■	■	■	■	■			■		■
	Collective						■			■		
Motivation	Personal	■					■	■				
	Economic	■	■	■	■	■		■				
	Ideological							■	■	■		
	Geo-political										■	■

Table 2 - de Bruijne et al.[48]

De Bruijne et al. are the first authors who introduced the attack scenario, also known as the kill chain in their typology. De Bruijne et al.'s threat actor typology is based not only on the hackers' motivations and skills, but also includes target, resource, and organization. Even though their typology was created for cyber security needs in the

[48] de Bruijne, M., van Eeten, M., Gañán, C.H. (2017). Towards a new cyber threat actor typology A hybrid method for the NCSC cyber security assessment. *Delft University of Technology - Faculty of Technology, Policy and Management.* https://repository.wodc.nl/handle/20.500.12832/2299.

Netherlands, they claim their new method is more relevant in today's world. They argue that by creating a structured analysis of cyber threat actors together with a structured approach on how to use a wider range of data, they lay a steppingstone for the creation of the most accurate typology. Finally, their hacker or threat agent categories are *extortionists, information brokers, crime facilitators, digital robbers, scammers and fraudsters, crackers, insiders, terrorists, hacktivists, state actors, and state-sponsored networks*. For the number of dimensions that distinguish these types of actors, a circumplex model is impossible to create and the data need to be depicted in a table form, in Table 2.[49]

1.3.2. Atkinson (2019)

Atkinson is yet another author from the field of cyber security. Nevertheless, he uses the methods of behavioural analysis and forensic psychology techniques to create new dimensions to better understand the processes, techniques, and skills of hackers. He stresses the importance of knowing "why", the understanding of the person behind the attacks and their motivation, as well as the "how" factors – the technical methods used in the malicious activities. Therefore, his model draws profiles of the threat actors according to four different metrics: *persistence, skill, greed, and stealth*. These attributes, which are not mutually exclusive are combined with other aspects such as the targeted industry, modes of attack (the techniques and methods used to different ends), identification (the actor's actions which help to identify specific actors), psychological models (their motivation to hack), remedy (the first actions needed to be taken after the attack), and proactive incidents response to create specific profiles based on each of the hacker categories Atkinson proposes. These profiles are supposed to facilitate clear incident response.[50]

For visualisation, Atkinson uses a four-circle Venn diagram with each hacker category. These diagrams do not have the same informative value as the other forms of visualisation created by other authors. Atkinson maybe makes up a new way to study the

[49] de Bruijne et al. (2017). Towards a new cyber threat actor typology A hybrid method for the NCSC cyber security assessment.

[50] Atkinson, S. (2019). Psychology and the hacker – Psychological Incident Handling. *SANS Institute.* https://www.scribd.com/document/461604555/psychology-hacker-psychological-incident-handling-36077.

hackers, however, if for example the skill and greed would be high, but persistence or stealth low, it is not possible to depict it in this type of diagram. Below is an example of the Venn diagram for the *Criminal.*[51]

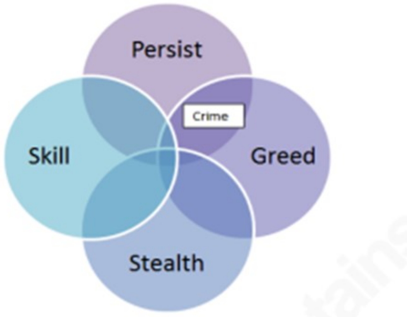
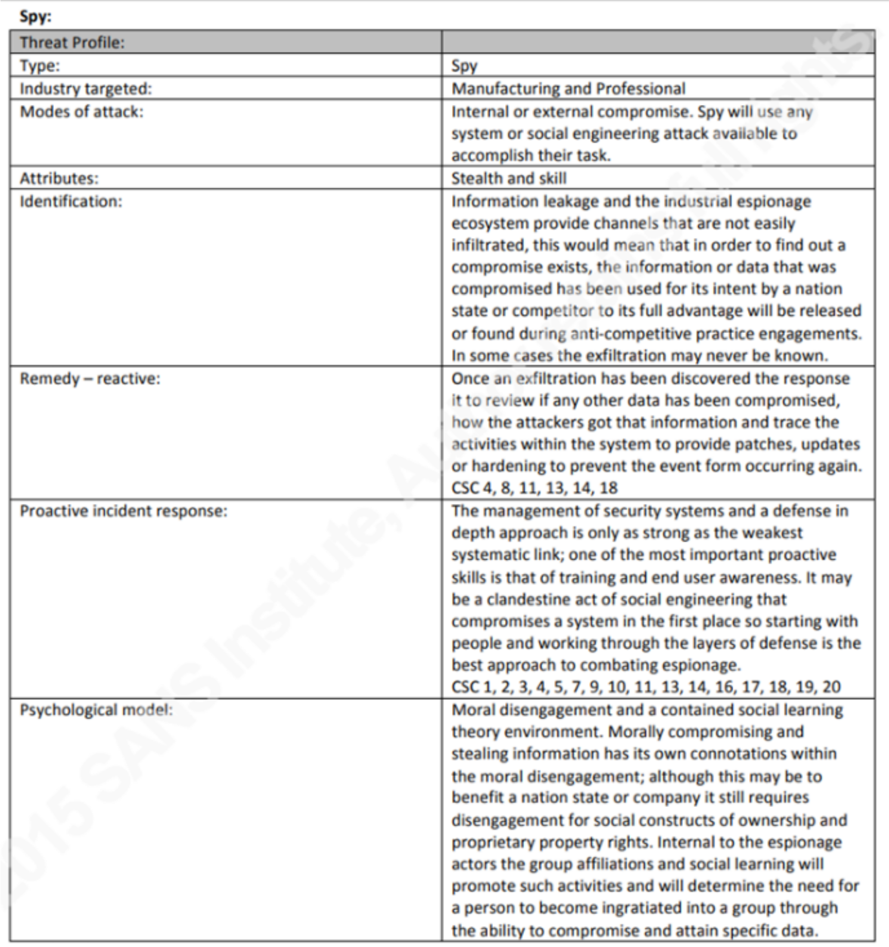


Fig. 6 - Atkinson's skill assessment of a criminal [52]

Probably for that reason, Atkinson also introduces separate tables for each of his six categories. In the tables, he includes the other aspects mentioned above in an exhaustive manner. Table 3 shows an example of the *Spy* category.

[51] Atkinson. (2019). Psychology and the hacker – Psychological Incident Handling.

[52] Atkinson. (2019). Psychology and the hacker – Psychological Incident Handling.



Spy:

Threat Profile:	
Type:	Spy
Industry targeted:	Manufacturing and Professional
Modes of attack:	Internal or external compromise. Spy will use any system or social engineering attack available to accomplish their task.
Attributes:	Stealth and skill
Identification:	Information leakage and the industrial espionage ecosystem provide channels that are not easily infiltrated, this would mean that in order to find out a compromise exists, the information or data that was compromised has been used for its intent by a nation state or competitor to its full advantage will be released or found during anti-competitive practice engagements. In some cases the exfiltration may never be known.
Remedy – reactive:	Once an exfiltration has been discovered the response it to review if any other data has been compromised, how the attackers got that information and trace the activities within the system to provide patches, updates or hardening to prevent the event form occurring again. CSC 4, 8, 11, 13, 14, 18
Proactive incident response:	The management of security systems and a defense in depth approach is only as strong as the weakest systematic link; one of the most important proactive skills is that of training and end user awareness. It may be a clandestine act of social engineering that compromises a system in the first place so starting with people and working through the layers of defense is the best approach to combating espionage. CSC 1, 2, 3, 4, 5, 7, 9, 10, 11, 13, 14, 16, 17, 18, 19, 20
Psychological model:	Moral disengagement and a contained social learning theory environment. Morally compromising and stealing information has its own connotations within the moral disengagement; although this may be to benefit a nation state or company it still requires disengagement for social constructs of ownership and proprietary property rights. Internal to the espionage actors the group affiliations and social learning will promote such activities and will determine the need for a person to become ingratiated into a group through the ability to compromise and attain specific data.

Table 3 - Atkinson's threat profile for Spy [53]

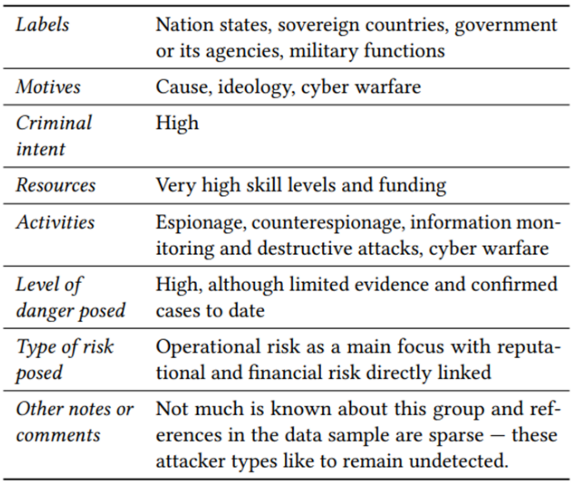
1.3.3. Moeckel (2019)

Another new taxonomy was created by Moeckel in 2019. Moeckel calls out the problems with the existing taxonomies and their updates, in particular arguing that they are based on previous works and literature rather than using new sets of data, as well as unclear justification and explanations on their use in threat modelling processes. It is important to note here that Moeckel uses data from digital banking-related cybercrimes. Therefore, in her taxonomy, Moeckel distinguishes 8 categories of hackers: *System challengers*, where she includes *white hat hackers, thrill seekers,* and *novices*; *Supporters*, who are not technically attackers themselves, rather they are the "money mules" that support real hackers; and *Insiders*; *Ideologists*, *Officials* (nation-states, governments,

[53] Atkinson. (2019). Psychology and the hacker – Psychological Incident Handling.

military); *Professionals I: groups and gangs; Professionals II: Small Groups and Individuals*; and *Toolkit users*. Each category then includes 7 to 9 distinguishing factors: whether there are subgroups to be found, their labels, motives, level of criminal intent, resources or skills, form of their activity, level of danger they possess, type of risk they pose, and "other notes and comments".[54] For visualisation Moeckel uses tables. Table 4 shows an example of the *Officials* category.

Table 4 - Moeckel' Officials



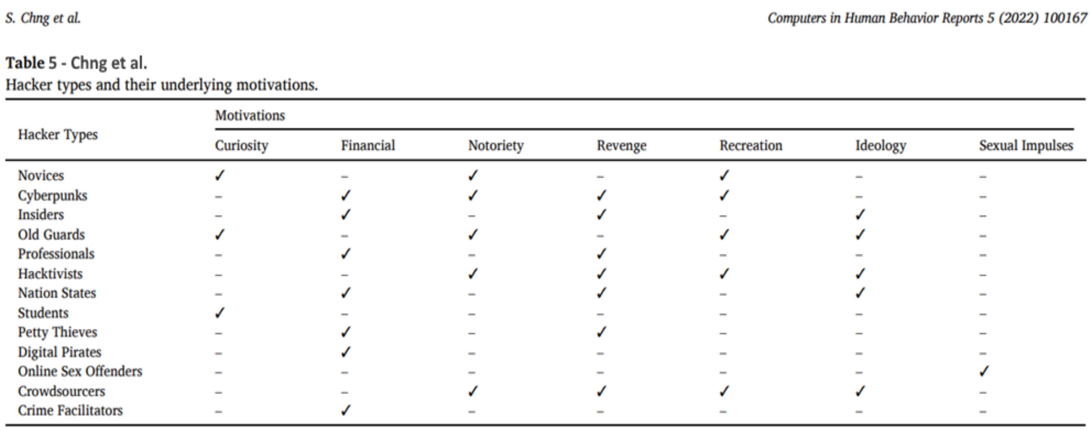
Labels	Nation states, sovereign countries, government or its agencies, military functions
Motives	Cause, ideology, cyber warfare
Criminal intent	High
Resources	Very high skill levels and funding
Activities	Espionage, counterespionage, information monitoring and destructive attacks, cyber warfare
Level 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.

[55]

[54] Moeckel, C. (2019). Examining and Constructing Attacker Categorisations: an Experimental Typology for Digital Banking. *Proceedings of the 14th International Conference on Availability, Reliability and Security (ARES '19) 93*, 1–6. https://dl.acm.org/doi/pdf/10.1145/3339252.3340341.

[55] Moeckel. (2019). Examining and Constructing Attacker Categorisations: an Experimental Typology for Digital Banking.

1.3.4. Chng et al. (2022)



S. Chng et al.

Computers in Human Behavior Reports 5 (2022) 100167

Table 5 - Chng et al.
Hacker types and their underlying motivations.

Hacker Types	Motivations						
	Curiosity	Financial	Notoriety	Revenge	Recreation	Ideology	Sexual Impulses
Novices	✓	–	✓	–	✓	–	–
Cyberpunks	–	✓	✓	✓	✓	–	–
Insiders	–	✓	–	✓	–	✓	–
Old Guards	✓	–	✓	–	✓	✓	–
Professionals	–	✓	–	✓	–	–	–
Hacktivists	–	–	✓	✓	✓	✓	–
Nation States	–	✓	–	✓	–	✓	–
Students	✓	–	–	–	–	–	–
Petty Thieves	–	✓	–	✓	–	–	–
Digital Pirates	–	✓	–	–	–	–	–
Online Sex Offenders	–	–	–	–	–	–	✓
Crowdsourcers	–	–	✓	✓	✓	✓	–
Crime Facilitators	–	✓	–	–	–	–	–

[56]

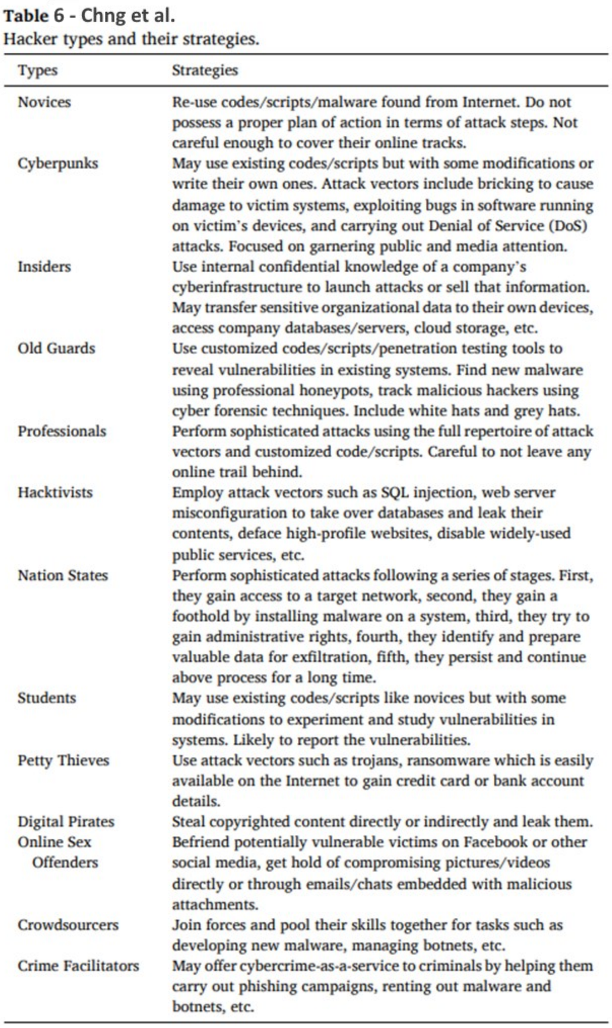


Table 6 - Chng et al.
Hacker types and their strategies.

Types	Strategies
Novices	Re-use codes/scripts/malware found from Internet. Do not possess a proper plan of action in terms of attack steps. Not careful enough to cover their online tracks.
Cyberpunks	May use existing codes/scripts but with some modifications or write their own ones. Attack vectors include bricking to cause damage to victim systems, exploiting bugs in software running on victim's devices, and carrying out Denial of Service (DoS) attacks. Focused on garnering public and media attention.
Insiders	Use internal confidential knowledge of a company's cyberinfrastructure to launch attacks or sell that information. May transfer sensitive organizational data to their own devices, access company databases/servers, cloud storage, etc.
Old Guards	Use customized codes/scripts/penetration testing tools to reveal vulnerabilities in existing systems. Find new malware using professional honeypots, track malicious hackers using cyber forensic techniques. Include white hats and grey hats.
Professionals	Perform sophisticated attacks using the full repertoire of attack vectors and customized code/scripts. Careful to not leave any online trail behind.
Hacktivists	Employ attack vectors such as SQL injection, web server misconfiguration to take over databases and leak their contents, deface high-profile websites, disable widely-used public services, etc.
Nation States	Perform sophisticated attacks following a series of stages. First, they gain access to a target network, second, they gain a foothold by installing malware on a system, third, they try to gain administrative rights, fourth, they identify and prepare valuable data for exfiltration, fifth, they persist and continue above process for a long time.
Students	May use existing codes/scripts like novices but with some modifications to experiment and study vulnerabilities in systems. Likely to report the vulnerabilities.
Petty Thieves	Use attack vectors such as trojans, ransomware which is easily available on the Internet to gain credit card or bank account details.
Digital Pirates	Steal copyrighted content directly or indirectly and leak them.
Online Sex Offenders	Befriend potentially vulnerable victims on Facebook or other social media, get hold of compromising pictures/videos directly or through emails/chats embedded with malicious attachments.
Crowdsourcers	Join forces and pool their skills together for tasks such as developing new malware, managing botnets, etc.
Crime Facilitators	May offer cybercrime-as-a-service to criminals by helping them carry out phishing campaigns, renting out malware and botnets, etc.

[57]

[56] Chng, S., Lu, Y. H., Kumar, A., Yau, D. (2022). Hacker types, motivations and strategies: A comprehensive framework. *Computers in Human Behaviour Reports.* https://www.sciencedirect.com/science/article/pii/S245195882200001X.

Chng et al. proposed a new framework by reviewing all the existing ones. Being the most exhaustive number of categories so far, the authors identified 13 types of hackers: *novices, students, cyberpunks, old guards, insiders, petty thieves, professionals, nation states, hacktivists, digital pirates, online sex offenders, crowdsourcers,* and *crime facilitators*; and 7 core motivations: curiosity, financial, notoriety, revenge, recreation, ideology, and sexual impulses. This updated framework, however, describes the distinct categories only in words and chooses tables to depict the motivations and strategies as seen in Table 5 and Table 6.[58]

1.4. Concepts in this thesis

Now that the background of hacker group categorizations has been introduced, it is possible to explain which typologies/taxonomies are going to be tested in this thesis. I decided to pick one framework from social sciences. Since the most updated taxonomy is from Seebruck, he created it based on the previous research, and it also encompasses the updated version of a circumplex model, which would add an interesting visual aspect to this thesis, I am choosing his framework to test as the one from social sciences.

The second taxonomy to test is de Bruijne et al.'s. The authors do not only include motivation and experience in their typologies. They expand the dimensions via which they categorize the hacker groups to the target, resources, and type of organization. De Bruijne et al. also utilize a table to depict the specific attributes of their threat actors. Therefore, I chose this typology to test since it is visibly different from those of social science researchers, and it is also the first framework in cyber security to categorize hacker groups.

The third typology I have chosen to test in this thesis is from Moeckel. It is different from the previous one since it focuses on motivation, criminal intent, resources, activities, level of danger and type of risk posed by the threat actors. Moeckel also chooses to depict the categories in a table, however, she utilizes separate ones for each of the actors, creating a new approach to the classification of hacker groups. That is the reason behind choosing this typology to test.

The last work from the field of studying hacker groups through a lens of cyber security I chose to test, is from Chng et al. It is the newest framework in this field and quite

[57] Chng et al. (2022). Hacker types, motivations and strategies: A comprehensive framework.

[58] Ibid.

interestingly, it distinguishes between the categories only based on their motivations, which the authors chose to visualize in a table form, and strategies, which are described only by word. It would be therefore useful to test whether this framework, although updated, is capable of proper classification since it includes only those two dimensions.

1.4.1. GIAC Threat Actor Profiling

Finally, to expand on the last dimension of studying hacker groups, I chose the Global Information Assurance Certification Paper from Stephen Irwin, in which he describes how to create a threat profile in praxis. Even though the entire process includes parts, which are not the focus of this paper, he also differentiates between threat actor characteristics creating five types of threat actors.

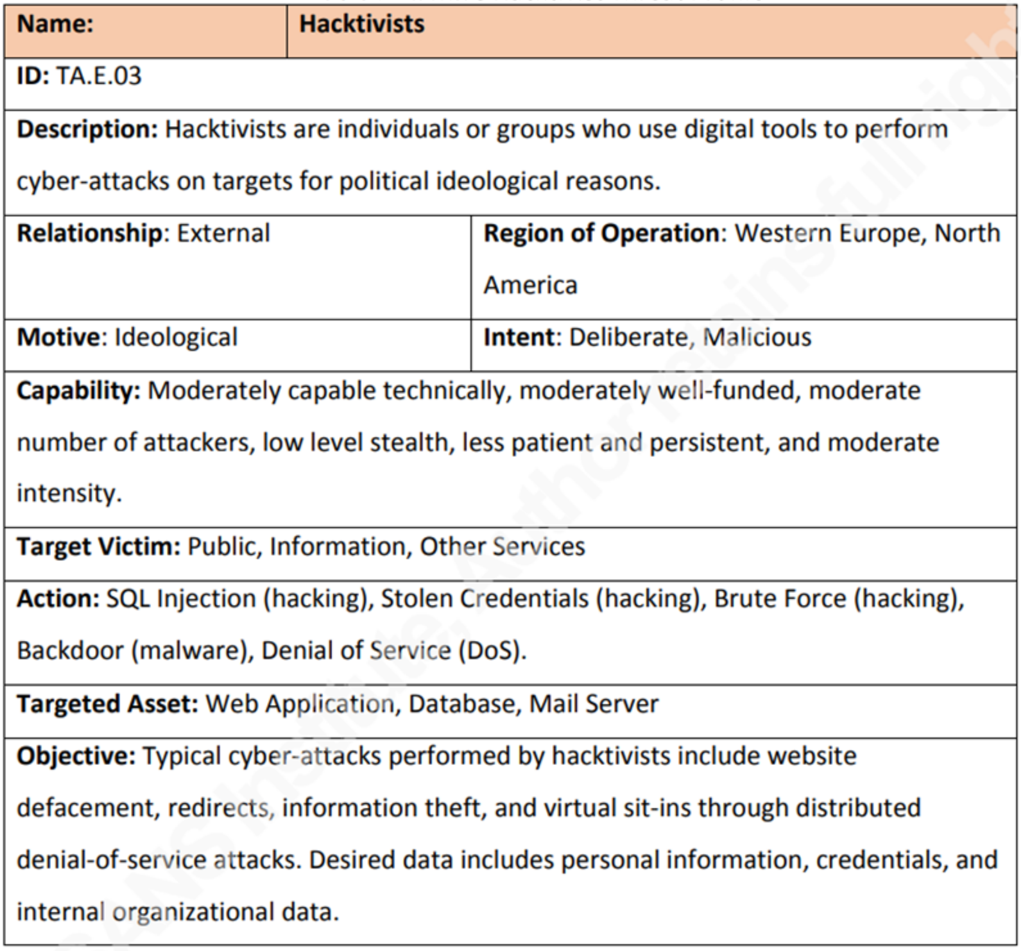
Irwin classifies distinct types of threat actors in a form of a table, giving them their Unique ID, Name, Description, and Relationship. Because Irwin's paper is aimed at organisations, this category is meant as a relationship to the organisation, distinguishing between *external* such as *cyber criminals, state-sponsored threat actors, or hacktivists; internal* meaning *system administrators, executives, managers,* and *end users;* and finally *partners* who represent third-party organisations that do business with the targeted institution. Furthermore, Irwin includes the Region of Operation as a dimension, which is meant as a geographic location of the threat actor, Motive including financial gain, espionage, ideological reasons, or no motive in an accidental incident. Moreover, there is Intent – deliberate/malicious/competitive/accidental reasons; Capability with various sub-attributes including "technical strength, financial support, political support, size, intensity, persistence (time), stealth (ability to hide), and access to a target."[59] Next, there is the Target victim, which describes the targeted industry according to the North American Industry Classification System (NAICS) for example; Action which involves tools and methods the attacker used; Target Asset meaning the list of assets that the threat actor tries to obtain or access; and finally Objective, which represents the ultimate asset the actor strives to access or compromise.[60]

[59] Irwin, S. (2014). Creating a Threat Profile for Your Organization. *Global Information Assurance Certification Paper.* https://www.giac.org/paper/gcih/1772/creating-threat-profile-organization/110995.

[60] Irwin. (2014). Creating a Threat Profile for Your Organization.

According to these dimensions, Irwin identifies *Cyber Criminals, State-sponsored Threat Actors, Hacktivists, System Administrators/End Users/Executives & Managers,* and *Partner.* As an example of the visualisation, I decided to include a table of the *Hacktivist* threat actor.[61]

Table 7 - Irwin's Hacktivist Threat Profile



Name:	**Hacktivists**
ID: TA.E.03	
Description: Hacktivists are individuals or groups who use digital tools to perform cyber-attacks on targets for political ideological reasons.	
Relationship: External	**Region of Operation**: Western Europe, North America
Motive: Ideological	**Intent**: Deliberate, Malicious
Capability: Moderately capable technically, moderately well-funded, moderate number of attackers, low level stealth, less patient and persistent, and moderate intensity.	
Target Victim: Public, Information, Other Services	
Action: SQL Injection (hacking), Stolen Credentials (hacking), Brute Force (hacking), Backdoor (malware), Denial of Service (DoS).	
Targeted Asset: Web Application, Database, Mail Server	
Objective: Typical cyber-attacks performed by hacktivists include website defacement, redirects, information theft, and virtual sit-ins through distributed denial-of-service attacks. Desired data includes personal information, credentials, and internal organizational data.	

[62]

1.5. Cases in this thesis

1.5.1. Shadow Brokers

The Shadow Brokers became infamous in 2016 when they released more than a gigabyte worth of tools allegedly belonging to one of the most secure organisations in the world, the American National Security Agency, Tailored Access Operation (TAO) unit, the Equation group. The Equation group itself is also covered in controversies. Even if they

[61] Ibid.

[62] Ibid.

did not accuse them directly, the Kaspersky Lab found out that the Equation group has connections to Stuxnet, the infamous worm that targeted Iranian's nuclear program, the Regin malware used to infect a state-owned Belgian firm Belgacom by the NSA, the Flame malware used for targeted cyberespionage in Middle Eastern countries, and many other highly sophisticated malware and espionage techniques. The Equation group is also known to target high-profile victims in a wide range of industries, ranging from military, diplomatic, and government, to finance, media, medical institutions, telecommunications, research institutions, and even Islamic scholars and many more, all together in 30 countries.[63]

The Shadow Brokers were able to steal the NSA's toolbox as well as highly sensitive information about its modus operandi. The hackers were active until 2017 and to this day, the world is questioning their identity as well as true motivations.[64] The lack of research on this group as well as their untraditional skills and method of working makes them a suitable candidate for testing the frameworks as it provides contrast with the other group, as well as represents a possible new type of actor. The details about the group are examined during the testing.

1.5.2. Fancy Bear

Since the activities of Fancy Bear are closely aligned with the strategic interests of the Russian government, the cybersecurity community agrees that the hacker group Fancy Bear is a Russian APT (advanced persistent threat) with affiliation to the Main Intelligence Directorate (GRU). The group is also known as APT28, Sofacy, Tsar Team, Pawn Storm, and many other names[65], and has been active since at least 2008.[66] The group became

[63] Gilbert, D. (2015). Equation Group: Meet the NSA 'gods of cyber espionage'. *International Business Times.* https://www.ibtimes.co.uk/equation-group-meet-nsa-gods-cyber-espionage-1488327.

[64] Valentová, A. (2022). Unveiling the Mystery Behind One of the Most Sophisticated Hacker Groups: Who are The Shadow Brokers?. *Security Outlines.* https://www.securityoutlines.cz/unveiling-the-mystery-behind-one-of-the-most-sophisticated-hacker-groups-who-are-the-shadow-brokers/.

[65] Secjuice. (2018). *Remember Fancy Bear?.* Secjuice. https://www.secjuice.com/fancy-bear-review/.

infamous in 2016 when it hacked the Democratic National Committee (DNC) and released sensitive information and emails to WikiLeaks in an attempt to influence the outcome of the 2016 U.S. presidential elections. However, the cybersecurity community has known the group for targeting governments, military, and security organisations specifically in the Caucasus region, Georgia, Ukraine, and NATO-aligned states. As for their methods, Fancy Bear uses mostly spear-phishing, zero-day exploits, and malware in their malicious activities.[67]

This group is suitable for testing as more research has been conducted about it. Since it is also operating for a longer time, it can be expected that the authors would have considered this type of actor and included it in their categorizations. The greater amount of information about this group thus gives an advantage in testing while also providing a nice contrast to the novel threat actor.

2. Testing the frameworks

The next part focuses on testing the carefully picked concepts and models based on the cases of The Shadow Brokers and Fancy Bear. The hacker groups are subjected to testing according to the typologies and dimensions the authors recognize within them. The important analysis of the hackers is conducted in the first section and utilized throughout the other typologies. Whenever there is a new aspect that the authors chose to research, the properties of the picked cases are studied in that particular section.

2.1. Seebruck's taxonomy and updated circumplex model

2.1.1. The case of The Shadow Brokers

2.1.1.1. Analysing The Shadow Brokers' motivations

The Shadow Brokers' first release in 2016 was about an auction of the stolen data. No one knew the hacker group yet, therefore their credibility was very low. Nevertheless, from the beginning throughout their activity, it is evident, that profit was one of the motivations of the group. They have tried auctioning, crowd-funding, and even developed

[66] Editorial Team. (2019). *Who is Fancy Bear (APT28)?.* Crowdstrike. https://www.crowdstrike.com/blog/who-is-fancy-bear/.

[67] TeamPassword. (2021). *Who is Fancy Bear and how can you protect yourself?.* TeamPassword. https://teampassword.com/blog/who-is-fancy-bear-and-how-can-you-protect-yourself.

a monthly dump service when the previous ways did not deem successful.[68] However, they did not only release the tools and data for money. Each time they dropped something and sometimes in between, they posted a message. It is possible to describe the group's way of thinking from the messages.[69]

In the first message, they have included a part addressed to "Wealthy Elites" where they accuse the elites of corrupting the legal system and bribing reporters to write in a positive manner about them. They connect the elites to politicians, and they mention the Equation Group while stressing that they "want make sure Wealthy Elite recognizes the danger cyber weapons, this message, our auction, poses to their wealth and control."[70] In the fifth message, they addressed the presidential elections in the United States, talking again about the elites and questioning the lack of media attention to their doing, which they have done several times before.[71] There other possible motivation can be spotted – prestige or notoriety.

Even though they mention in one of the messages, where they express their anger about a lack of buyers and threaten to stop selling altogether, that they were always only after money and "Free dumps and bullshit political talk was being for marketing attention"[72], their next message included political ideas again. They addressed the American people, specifically President Trump in detail, and mentioned many other issues such as globalism, white privilege, Russia, and the so-called deep state (a secret group of people controlling and manipulating the US government policy), showing vast knowledge of the American politics as well as many international issues.[73]

[68] Suiche, M. (2017). *The Shadow Brokers Cyber Fear Game-Changers.* Comae technologies. https://archive.org/details/us-17-Suiche-TheShadowBrokers-Cyber-Fear-Game-Changers-wp.

[69] The Shadow Brokers' Steemit Messages archive. https://swithak.github.io/SH20TAATSB18/Archive/Messages/TSB/TheShadowBrokers-SteemitMessages/.

[70] The Shadow Brokers. (2016). *Message#1*. Steemit. https://swithak.github.io/SH20TAATSB18/Archive/Messages/TSB/Message1/

[71] The Shadow Brokers. (2016). *Message#5*. Steemit. https://swithak.github.io/SH20TAATSB18/Archive/Messages/TSB/Message5/

[72] The Shadow Brokers. (2017). *Message#8*. Steemit. https://swithak.github.io/SH20TAATSB18/Archive/Messages/TSB/Message8/.

[73] The Shadow Brokers. (2017). *Message#9*. Steemit. https://swithak.github.io/SH20TAATSB18/Archive/Messages/TSB/Message9/.

This raises a question of The Shadow Brokers being an Equation group (American) insider seeking revenge. In Message #10 while denigrating Snowden, they posted “TheShadowBrokers is not running, America is our fucking country and we staying and fighting for it!”.[74] It is plausible that the group is American for one more reason. Their ideology can be summarized as enlarging transparency, similarly to the cypherpunk ideology (advocating widespread use of strong cryptography and privacy-enhancing technologies as a means to social and political change; an ideology Julian Assange from WikiLeaks subscribes to[75]), while disadvantaging, or maybe even overthrowing the allegedly corrupt elites. Therefore, there is a plausibility for one of their motives to be revenge, since revengeful are usually the employees feeling underappreciated or the fired ones. Take Snowden, for example, he found out the truth about the National Security Agency, which was clashing with his idealizations of the US and decided to publish their secrets.[76]

There is even more evidence supporting this theory. The first one is the language of their Steemit (a blockchain-based blogging and social media website) messages. The writer Franceschi-Bicchierai did a linguistic analysis of their messages and concluded that they are intentionally inserting errors and adjusting their writing to sound like a foreigner. Nevertheless, the author is a native English speaker.[77] However, even though I completely agree that the group is purposely trying to sound foreign, I believe, someone with great English skills, and not necessarily a native speaker, could achieve the same objective.

The second evidence was already mentioned, their thorough knowledge of American politics. The fact that they openly share their opinions about international relations and specific political opinions, such as advising Donald Trump f.e., decreases the probability of this group being an APT since it is not usual for them to present an

[74] The Shadow Brokers. (2017). *Message#10.* Steemit. https://swithak.github.io/SH20TAATSB18/Archive/Messages/TSB/Message10/.

[75] Greenberg, A. (2013). *This Machine Kills Secrets: Julian Assange, the Cypherpunks, and Their Fight to Empower Whistleblowers.* Plume.

[76] Valentová, A. (2021). Decisions Behind the Biggest Leaks in History: What Motivates a Leaker?. *Security Outlines.* https://www.securityoutlines.cz/the-prototypical-leaker/.

[77] Franceschi-Bicchierai, L. (2016). The NSA Data Leakers Might Be Faking Their Awful English To Deceive Us. *Vice.* https://www.vice.com/en/article/gv5d93/the-shadow-brokers-nsa-leakers-linguistic-analysis.

ideological link to their supervisors unless they are trying to hide their identity and talk ideologically while posing as someone else. Furthermore, The Shadow Brokers even seem to have an exceeding knowledge of the American culture due to the high number of cultural references posted in their messages.[78]

On top of these, there is more proof. A former NSA employee, who, however, stayed anonymous, claimed that he and his colleagues believe that there was no hack, nor are The Shadow Brokers a group of people, but rather an individual. He stated that some of the files and scripts that the hackers were selling were only accessible internally, stored on a physically separated network, which is not at all connected to the internet and there is no reason for this data to be on a server someone would choose to hack.[79] This claim was backed by a cybersecurity expert, Matt Suiche, who analysed the hacker group as well. He said that something from the stolen toolkit was indeed stored on a separate network with no internet access and it would not be logical to store some of the stolen scripts elsewhere since they are only used for setting up a workstation pre-operation. Furthermore, he noted, that the hierarchy of the files and their unchanged naming look like they were copied directly from the source.[80] On top of that, The Shadow Brokers mentioned names of multiple projects that have not been included in the stolen data.[81]

Most importantly, the insider theory supports the fact that even the NSA itself suspected The Shadow Brokers to be an insider. They have arrested two men Harold T. Martin III, an NSA contractor working through Booz[82] (which is by the way the same organisation Snowden was working for)[83] because they found terabytes of stolen material

[78] The Shadow Brokers‘ Steemit Messages Archive.

[79] Cox, J. (2016). Former NSA Staffers: Rogue Insider Could Be Behind NSA Data Dump. *Vice*. https://www.vice.com/en/article/ezp5na/former-nsa-staffers-rogue-insider-shadow-brokers-theory.

[80] Suiche, M. (2016). Shadow Brokers: The insider theory. *Medium*. https://medium.com/comae/shadowbrokers-the-insider-theory-ded733b39a55#.br7pbm7ar.

[81] Darknet Diaries podcast. *EP 53: SHADOW BROKERS.* Darknet Diaries. https://darknetdiaries.com/transcript/53/.

[82] Morse, D. and Jackman, T. (2019). NSA contractor sentenced to nine years in theft of massive amounts of classified material. *The Washington Post*. https://www.washingtonpost.com/local/public-safety/nsa-contractor-who-stole-massive-amounts-of-classified-material-set-for-sentencing-friday/2019/07/18/83f1bf96-a995-11e9-9214-246e594de5d5_story.html.

[83] Suiche. (2017). The Shadow Brokers Cyber Fear Game-Changers.

at his home. Martin was not found guilty, however, the time frame when the arrest happened seems very suspicious. Even more so due to the other arrested person, Nghia Hoang Pho, an employee of TAO, who was sentenced to prison for wilful retention of classified material. Even though the hearing was classified, the Director of the NSA, Michael S. Rogers, sent a public letter to the court regarding this case. According to the analysis of the letter, there are some indications of the retained data including class exploits such as Eternal and the FuzzBunch framework, which The Shadow Brokers published.[84] The Shadow Brokers have also been silent since 2017, and even though they also did not publish their material for 2 years while they had it before, and they may be doing the same thing now, it is also possible that the insider of TAO has been caught and the news just did not leak to media due to the NSA trying to preserve its reputation.

Lastly, a minor but interestingly comical connection can be made to the insider theory. According to Suiche's claims, there is supposed to be a great gaming culture inside the TAO group.[85] The name of The Shadow Brokers was most probably inspired by a game called Mass Effect, where the character represents an enigmatic figure at the head of an expansive organization which trades in information and is always selling to the highest bidder"[86].

Some of the evidence supporting the insider theory shows that the group also very often tends to promote an ideology. The Shadow Brokers shared their political ideas, inclinations and anti-globalist and anti-war perspectives many times through their messages.[87] It is therefore important to consider ideology being one of the main motivations of the group as well.

In conclusion, the main motivation of The Shadow Brokers is probably profit. The secondary motivation could be ideology due to the number of opinions promoted by the group. However, these opinions could be also fuelled by a need to take revenge because there is a lot of evidence connecting The Shadow Broker to a TAO insider person/people. Nevertheless, the group did not only focus on the Equation Group in their slander, but they also expressed many other opinions about political issues, specifically American ones, therefore, ideology seems like a stronger motive than seeking revenge. Lastly, even the

[84] SH20TAATSB18. *Case Updates*. SwitHak.https://swithak.github.io/SH20TAATSB18/about/.

[85] Suiche. (2016). Shadow Brokers: The insider theory.

[86] Mass Effect Wiki. *Shadow Broker*. https://masseffect.fandom.com/wiki/Shadow_Broker.

[87] The Shadow Brokers' Steemit Messages Archive.

prestige motive cannot be absolutely ruled out as one of the motivators since the pride they have taken in managing to steal the data was evident.

2.1.1.2. *Fitting the case to the framework*

Seebruck bases his types of hackers on Roger's and Meyers et al.'s typologies. The categories are *novices, crowdsourcers, punks, hacktivists, insiders, criminals, coders, and cyber warriors.* Using the elimination method, the category of *novices* can be eliminated firstly since the skill of this type is depicted as very low and the Equation group is regarded as one of the most, if not the most sophisticated hacker groups in existence.[88] Therefore, hacking into such an organisation would require a significantly high skill level. By this logic, the *punks, as well as the crowdsourcers,* can be eliminated as well due to their sophistication being quite low. Moreover, The Shadow Brokers have not participated in any kind of crowdsourcing activity.[89]

The next type which can be easily discarded is the *coders,* by previous typologies known as the "white hat hackers" because their motivations do not include seeking profit, which The Shadow Brokers clearly did.[90] The *hacktivists* can be disposed of as a type for the same reasons. Seebruck does not see profit as any of their motivations.[91]

Finally, although *criminals* are primarily motivated by profit and secondary by revenge, which could be the case of The Shadow Brokers, Seebruck recognizes their skill set as upper-intermediate, which is almost certainly not enough to hack one of the most sophisticated organisations in the world and stay unnoticed for two years, which was the case here.[92]

This leaves us with the types of *insiders and cyber warriors.* Profit is seen as the second motivation for both types, which could be plausible in this case. And i*nsiders'* primary motivation is estimated to be revenge, while the primary motivation of *cyber*

[88] Paganini, P. (2015). The Equation Group shows most complex and sophisticated hacking techniques ever seen. *Security Affairs.* https://securityaffairs.co/wordpress/33637/cyber-crime/the-equation-group-atp.html.

[89] The Shadow Brokers' Steemit Messages Archive.

[90] Ibid.

[91] Seebruck. (2015). A typology of hackers: Classifying cyber malfeasance using a weighted arc circumplex model.

[92] Suiche. (2016). Shadow Brokers: The insider theory.

warriors is ideology. And while *cyber warriors* are proposed to have more sophisticated skills, if The Shadow Brokers were a case of *insiders* from the TAO, their skillset would probably be of the same excellence as the *cyber warriors'*.

However, according to Seebruck's taxonomy, the group cannot be *insiders* because they would not show signs of ideology or prestige. The only plausible category would therefore be *cyber warriors,* however, there are multiple issues even here. Firstly, The Shadow Brokers expressed their pride in being able to hack one of the most secure organisations in the world, and the *cyber warriors,* according to Seebruck, are not supposed to do that. Furthermore, even if this category was motivated by ideology, it is not quite common for the APTs to post their ideas for the entire world to see, purely for the reason of attribution, to make it harder to connect them to a state actor.

The Shadow Brokers, therefore, do not fit precisely into Seebruck's hacker categories. The ideological talk, even if it would be for the purpose of commercializing the data for sale, is stronger than the possibility of being motivated by revenge. It is even possible that while probably being an insider, revenge in its typical meaning is not at all a motivator for the group. For The Shadow Brokers, therefore, Seebruck's taxonomy is not applicable. Nevertheless, it is still possible to use his updated weighted arc circumplex model to depict this specific case. The model would look like Figure 7.

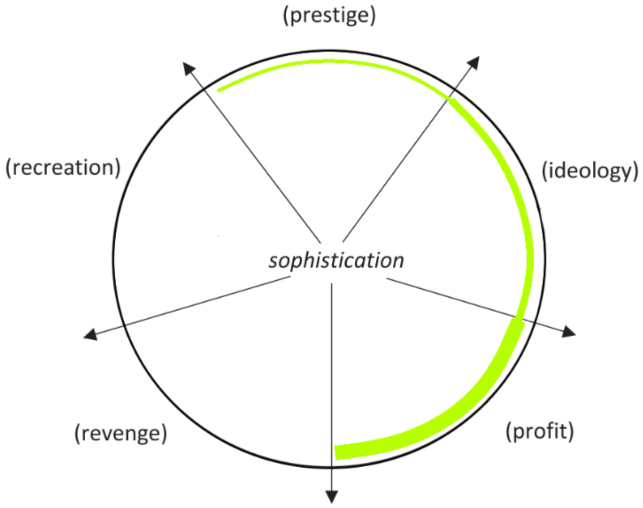


Fig. 7 - The Shadow Brokers circumplex model according to Seebruck's typology

It is important to note that The Shadow Brokers are an extremely specific group of hackers that are recognized to have a sort of bizarre modus operandi. Before evaluating Seebruck's taxonomy it is, therefore, necessary to test it on another hacker group, which is more known and more classical in a sense of hacker group categorizations. It is also suspected that this group is a Russian APT, therefore it should fit the test of the *Cyber warriors* category of Seebruck's taxonomy very nicely.

2.1.2. The case of Fancy Bear

As was already mentioned, Fancy Bear's targets go suspiciously hand in hand with the strategic interests of Russia. It attacks mostly the Transcaucasian region, Georgia, Ukraine, and NATO-aligned states. The group is accused of hacking the German and Norwegian parliaments, a French television station TV5Monde, the White House and the DNC, and companies such as the US defense contractors Academi, Science Applications International Corporation (SAIC), Boeing, Lockheed Martin, NATO, the Organization for Security and Co-operation in Europe (OSCE), Macron's presidential candidacy campaign, and even more. Amongst the targets were, however, also some Russian citizens and individuals of other nationalities as well, most notably the former oil tycoon Mikhail Khodorkovsky, and Maria Alekhina of the band Pussy Riot. Moreover, on April 15, 2016, which is a day to celebrate the holiday honouring the military's electronic warfare service in Russia, and which also was around the time of the DNC hack, the group was suspiciously inactive. Moreover, after Russian athletes were banned from the 2016 Rio Olympics, Fancy Bear attacked the World Anti-Doping Agency (WADA). [93]

In sum, a lot of evidence points to a Russian APT. According to Seebruck's taxonomy, Fancy Bear would most likely fall under the category of *cyber warriors,* indicating a high level of skills and primary motivation ideology. However, this category is also supposed to look for profit as a secondary but still very strong motivation, which Fancy Bear has never done.[94] It could be also said that the attack in 2016 on the World Anti-Doping Agency (WADA) was motivated by revenge since the hackers attacked the agency after some Russian athletes were banned from the Olympic games after finding state-sponsored doping.[95] However, the revenge would probably be driven by an ideology, therefore I would still include it into the ideology motivation.

[93] TeamPassword. (2021). Who is Fancy Bear and how can you protect yourself?.

[94] Ibid.

[95] WADA. (2016). *Cyber Security Update: WADA's Incident Response*. WADA. https://www.wada-ama.org/en/news/cyber-security-update-wadas-incident-response.

Nevertheless, Seebruck's weighted arc circumplex model could be also used for the Fancy Bear hacker group, even though the result would be a little underwhelming due to only one visible motivation of the group as seen below.

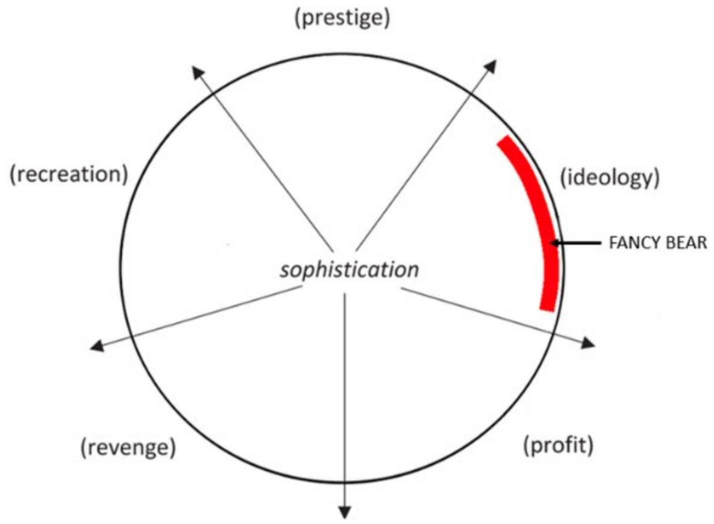


Fig. 8 - FANCY BEAR circumplex model according to Seebruck's typology

2.2. de Bruijne et al. taxonomy

2.2.1. The Shadow Brokers

To test this framework, the most feasible way would be to follow the table to find out which category, if any, is suitable for the case of The Shadow Brokers. Firstly, the table considers the target. As was mentioned in the thesis, The Shadow Brokers had at least from what is known, only one target, the Equation Group, from TAO, NSA. From the types of targets available in this taxonomy, the public sector fits the most. Secondly, the level of expertise is unquestionably high since The Shadow Brokers managed to hack one of the most skilled organisations in the world and stayed unnoticed for two years. Thirdly, there is the level of resources. De Bruijne states that the level of resources is high when the attacker can conduct DDoS attacks, for example with the case of Stuxnet, or when the attack on the Ukrainian electricity grid happened. The resources were labelled as high since the breach has been present for a long time before the actual attack took place.[96] Based on this logic, The Shadow Brokers' resources would fit this level since they spent

[96] de Bruijne et al. (2017). Towards a new cyber threat actor typology A hybrid method for the NCSC cyber security assessment.

two years going through the data before they published them, and no one knows how they got to them.

Next is the dimension of Organisation. Though The Shadow Brokers may be an individual, it could also be a group of people. They seemed to have a clear vision of their doing throughout the whole time of their activity, therefore, it is derivable that the group is very stable. That would point to The Shadow Brokers being a single entity, with a clear command structure. It would be also possible that the group has more collaborative relationships. In de Bruijne et al.'s terms, The Shadow Brokers could therefore be either a Hierarchy or a Network. According to the authors, the motivations are unintentional, personal, economical, ideological, and geopolitical. Interestingly, the authors distinguish between ideological and geopolitical. A geo-political is described as trying to improve a state's position in relation to its allies, neutrals, or enemies. With ideological motivation, there is supposed to be a message or goal central to the group's doing. As was described above, the probable primary motivation of The Shadow Brokers is profit-seeking. However, secondary comes ideology with the possibility of personal revenge as another motivator due to empirical evidence.

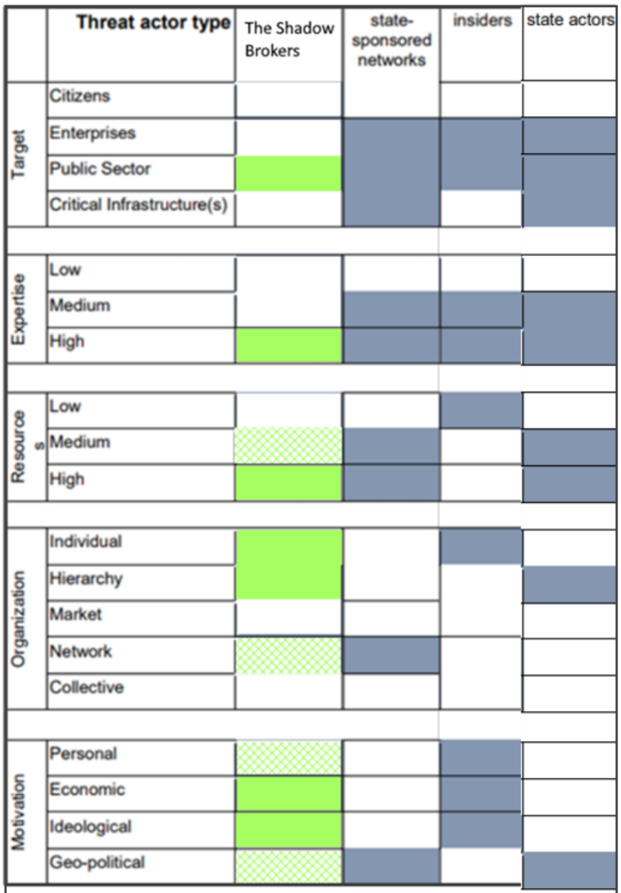
Nevertheless, geopolitical motivation also cannot be completely discarded. It was questioned if The Shadow Brokers are a state-sponsored APT. I have analysed these questions in an article, where I considered the most probable state actors that would target the United States, specifically NSA's TAO. Firstly, I examined China. There is some evidence eliminating the possibility. Obama came to office in 2015 and threatened Xi Jinping with sanctions after the Chinese hacked the U.S. Office of Personnel Management. Chinese hackers have been silent after that for 18 months. More importantly, however, one Chinese-affiliated group called APT31 was already in possession of a clone of the NSA's exploit EpMe with a Windows zero-day bug. They had it for four years before The Shadow Brokers became active. It would not make sense for an APT to release a tool usable for them, since once public, the systems could be protected from exploitation. The same logic could be applied to all APT suspicions. It would be more beneficial for them to keep it and use it in secret, rather than release it. Furthermore, China is currently one of the richest nations. Seeking profit in this manner seems rather unreasonable. Secondly, North Korea was discarded since The Shadow Brokers published two posts making fun of the country, specifically Kim Jong Il, the country's political regime and ideology. It is highly unlikely that the hackers from North Korea would do that.[97]

If The Shadow Brokers were a state-sponsored APT, they would probably be Russian. The relations between the United States and Russia aid this theory since after Russia was publicly accused of middling in their elections, the Shadow Brokers started releasing. They also share the same opinion with Russia about the war in Syria. The group has mentioned they were against intensifying the U.S. involvement and were disappointed in Trump, whom they have supported before, for doing such a thing. Even Edward Snowden pointed to the possibility of a new cyber cold war. It is also probable that Russia wants the NSA to seem incompetent. However, it would still make more sense for it to keep the valuable data. Even more so with the fact that they have stolen information about NSA agents, a piece of critical classified information.[98]

Nevertheless, the possibility of The Shadow Brokers being a state-sponsored APT is not entirely disprovable, as well as the geopolitical motivation. Even de Bruijne et al. mention The Shadow Brokers in their study as an example of a State-sponsored network. Describing them as a state-affiliated group that is organised in a network form. According to the analysis, I depicted the Shadow Brokers case in de Bruijne et al.'s Table 8 next to the *state-sponsored network*, *state actors* and *insider* category. I have decided to hatch the less likely options for The Shadow Brokers. If we were to consider the evidence pointing to the insider theory, where the resources are low since only one person is operating, the *insider* would be the most fitting category. Nevertheless, The Shadow Brokers have again proven to be a very unconventional group that does not necessarily fit into yet another taxonomy.

[97] Valentová, A. (2022). Unveiling the Mystery Behind One of the Most Sophisticated Hacker Groups: Who are The Shadow Brokers?.

[98] Ibid.



	Threat actor type	The Shadow Brokers	state-sponsored networks	insiders	state actors
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 8 - The Shadow Brokers according to de Bruijne et al.'s taxonc

2.2.2. Fancy Bear

Now let us look at the properties of Fancy Bear according to de Bruijne et al. More research has been done about this threat actor so it should be easier to pinpoint them to a specific category. The authors themselves mention them in their study when they called out the previous typologies of missing out on the newly emerging trends in the last few years. They said that the previous works do not include a type that stands for private actors that are presumably recruited for state-sponsored attacks. Therefore, they would probably put them again into the state-sponsored type of actor. To verify that assumption, the target is to be described firstly. The group has targeted the band Pussy Riot, journalists, political figures (mainly Russian and Ukrainian opposition), U.S. intelligence employees, the chairman of Clinton's campaign, John Podesta and more than 130 democrats.[99] Easy to

[99] Associated Press. (2017). Russian hackers hunted journalists in years-long campaign. *Star Advertiser.* https://www.staradvertiser.com/2017/12/22/breaking-news/russian-hackers-hunted-journalists-in-years-long-campaign/.

say, citizens were one of the targets. Furthermore, there were the already mentioned attacks on the French television, WADA, and the International Olympic Committee, German and Norwegian Parliament, Dutch ministries, and even the Czech Ministry of Foreign Affairs[100], representing the enterprises and public sector. The financial institutions, which were supposed to be targeted as well,[101] fall under the category of critical infrastructure. Therefore, even if Fancy Bear does not primarily attack critical infrastructure, such as the Voodoo Bear attack on the Ukrainian energy companies,[102] for example, this category cannot be completely discarded.

Secondly, their level of expertise is probably very high since they mostly employ spear-phishing attacks, in which they customise the communication to target specific individuals or organisations, and zero-day exploits. In a zero-day exploit, the attacker exploits the vulnerabilities of software intending to add malware into programs, data, or computer networks. It is a very sophisticated form of attack, and the Fancy Bear group are believed to be one of the most successful actors at deploying these attacks.[103] Thirdly, their resources are again very high since they are able to run multiple extensive intrusion operations at the same time[104] and they had targets in at least 32 nations.[105]

Furthermore, de Bruijne et al. mention the group in their research also as an example of a network of attackers, where they assume that they are consistently recruited to carry out state-sponsored activities. That is possible since as mentioned above, they sometimes run many operations at once. Nevertheless, they could also have a hierarchy established inside of the group. Even more so, when the fact that they could be a GRU Unit

[100] iDnes. (2019). Kyberútok na českou diplomacii způsobil cizí stát, potvrdil Senátu NÚKIB. *iDnes.* https://www.idnes.cz/zpravy/domaci/kyberutok-ceska-diplomacie.A190813_141319_domaci_vlc.

[101] Palenik, L. (2015). *Russian hacking group APT28 planned attacks against global banks*. We live security. https://www.welivesecurity.com/2015/05/14/russian-hacking-group-apt28-planned-attacks-global-banks/.

[102] Cybersecurity Help. (2022). *The story of the four bears: Brief analysis of APT groups linked to the Russian government.* Cybersecurity Help. https://www.cybersecurity-help.cz/blog/2507.html.

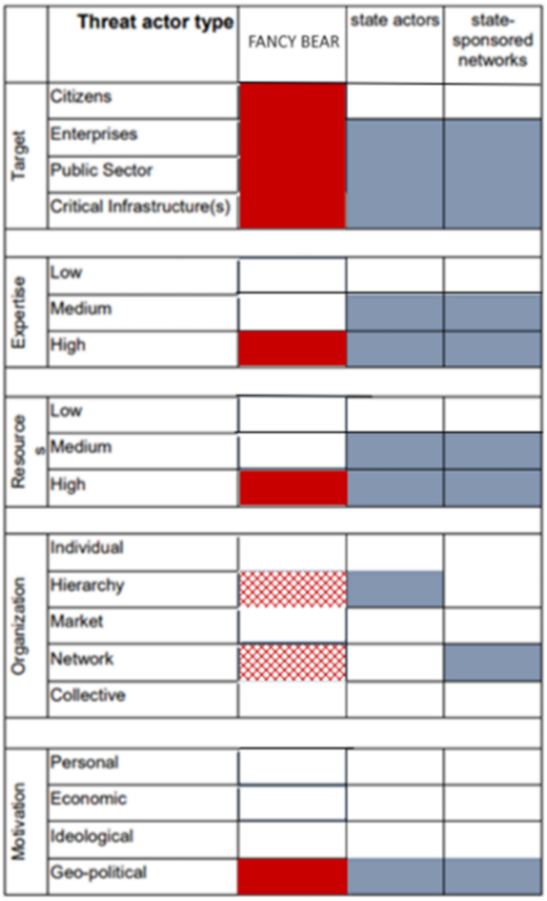
[103] TeamPassword. (2021). Who is Fancy Bear and how can you protect yourself?.

[104] Editorial Team. (2019). Who is Fancy Bear?.

[105] Crowdstrike. *Fancy Bear*. Crowdstrike. https://adversary.crowdstrike.com/en-US/adversary/fancy-bear/.

26165, which the United States believe in[106], is considered. There is not enough data to exclude one of the categories. As for their motivation, according to de Bruijne et al., the geo-political motivation is "trying to improve the position of a state-actor",[107] which Fancy Bear is doing based on all the facts.

In conclusion, the Fancy Bear group meets all criteria to fall under the category of *state actors*, apart from targeting individuals. However, with the same exception, it would also meet all criteria in *state-sponsored networks* since we do not know if the group is organized hierarchically or is more of a network type. The findings are visible in Table 9.



	Threat actor type	FANCY BEAR	state actors	state-sponsored networks
Target	Citizens	🟥		
	Enterprises	🟥	🟦	🟦
	Public Sector	🟥	🟦	🟦
	Critical Infrastructure(s)	🟥	🟦	🟦
Expertise	Low			
	Medium		🟦	🟦
	High	🟥	🟦	🟦
Resource s	Low			
	Medium		🟦	🟦
	High	🟥	🟦	🟦
Organization	Individual			
	Hierarchy	▨	🟦	
	Market			
	Network	▨		🟦
	Collective			
Motivation	Personal			
	Economic			
	Ideological			
	Geo-political	🟥	🟦	🟦

Table 9 - FANCY BEAR ac. to de Bruijne et al.'s typology

[106] Cybersecurity Help. (2022). The story of the four bears: Brief analysis of APT groups linked to the Russian government.

[107] de Bruijne et al. (2017). Towards a new cyber threat actor typology A hybrid method for the NCSC cyber security assessment.

2.3. Moeckel's framework

2.3.1. The Shadow Brokers

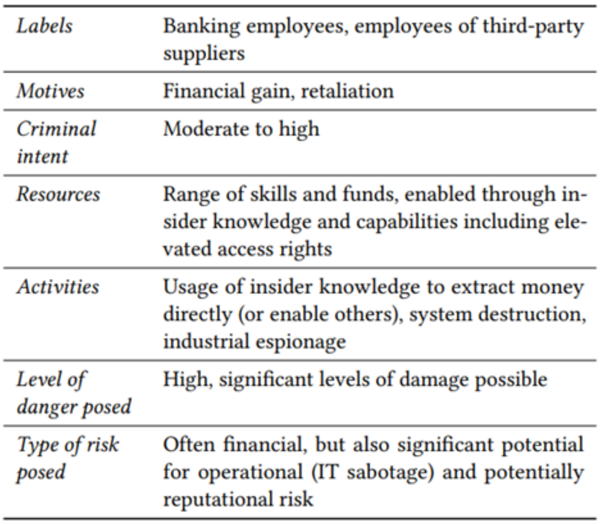
Moeckel uses separate tables for every hacker category. In each, there are metrics which we could compare to the case of The Shadow Brokers. Firstly, there are *Motives,* with this case it was already established that money, ideology with the possibility of retaliation, and even notoriety are the motivations of this group. Secondly, *Criminal intent* is unquestionably high. *Resources* are defined as time, finances, technical skills and capabilities, initial access options, insider knowledge or personal connections available to the attacker.[108] In the case of The Shadow Brokers, it is not possible to find out their level of funding. It is not refutable that they would be a state-sponsored APT, therefore showing a high level of funding. However, they could also be an insider with a low level. What is certain though, is their high skill level. It is also not known how exactly they reached the NSA's servers. Some experts believe that they found one of the NSA's tools hidden on the internet and hacked it to reach access. However, they also question the contingency that someone would randomly find the cache without looking.[109] Next is the *Level of danger posed*. With being able to hack the NSA and having no issues with releasing its classified information, it is presumable that the level is very high. And lastly, the *Type of risk posed* is in this case reputational and operational.

According to Moeckel's tables, The Shadow Brokers fit mostly into the categories of *Insiders, Professionals I: groups or gangs, Professionals II: Small groups and Individuals,* and *Ideologists.* Nevertheless, since both categories of professionals are supposed to be motivated solely by financial gain, more probable are the categories of *Insiders,* who however miss the ideological motivation, and *Ideologists*, who Moeckel states, could be also motivated by financial gain but it is usually a secondary motive. The Shadow Brokers' table based on Moeckel's categorization is seen in Table 12.

[108] Moeckel. (2019). Examining and Constructing Attacker Categorisations: an Experimental Typology for Digital Banking.

[109] Schneier, B. (2017). Who Are the Shadow Brokers?. *The Atlantic.* https://www.theatlantic.com/technology/archive/2017/05/shadow-brokers/527778/.

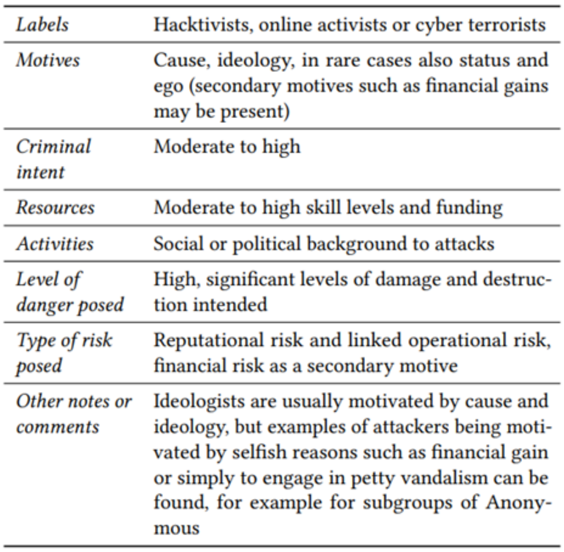
Table 10 - Moeckel's Insider



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

[110]

Table 11 - Moeckel's 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 12 - The Shadow Brokers according to Moeckel's typology

Motives	Financial gain, ideology, retaliation, (notoriety)
Criminal Intent	High
Resources	High skill levels with possible insider knowledge; Funding is unknown
Activities	Server hacking with the intention of leaking classified information possibly for a profit
Level of danger posed	High, significant level of damage intended
Type of risk posed	Reputational, operational

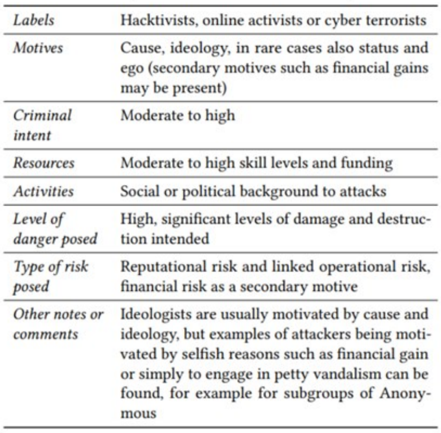
2.3.2. Fancy Bear

For Fancy Bear the motives could be labelled as ideology, or/and cyber warfare. Their criminal intent is high, and resources both skills and funding high as well, the

[110] Moeckel. (2019). Examining and Constructing Attacker Categorisations: an Experimental Typology for Digital Banking.

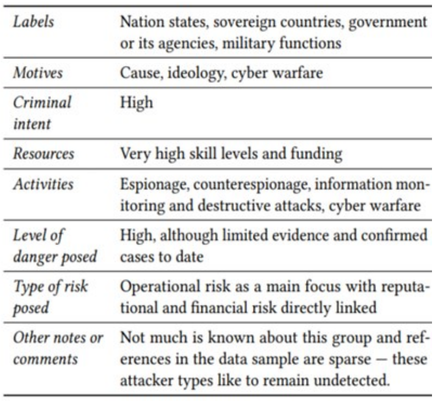
activities of Fancy Bear include spear-phishing and zero-day exploits as was mentioned above, mainly they leak information with the aim of discrediting Russian adversaries, and sometimes they destroy systems to create instability and hide behind an identity of other threat actors such as the Islamic State, for example.[111] They pose a high level of danger, even if they do not target critical infrastructure, they are probably capable to do so. And they present mainly reputational and operational risks indirectly linked to financial danger. The most suitable categories according to Moeckel would therefore be *Ideologists* or *Officials.* Although the author states that *Officials* usually like to stay undetected. The table for Fancy Bear compared to the other two is shown below and in Table 13.

Table 11 - Moeckel's 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 12 - Moeckel's 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.

[112]

Table 13 - Fancy Bear according to Moeckel's typology

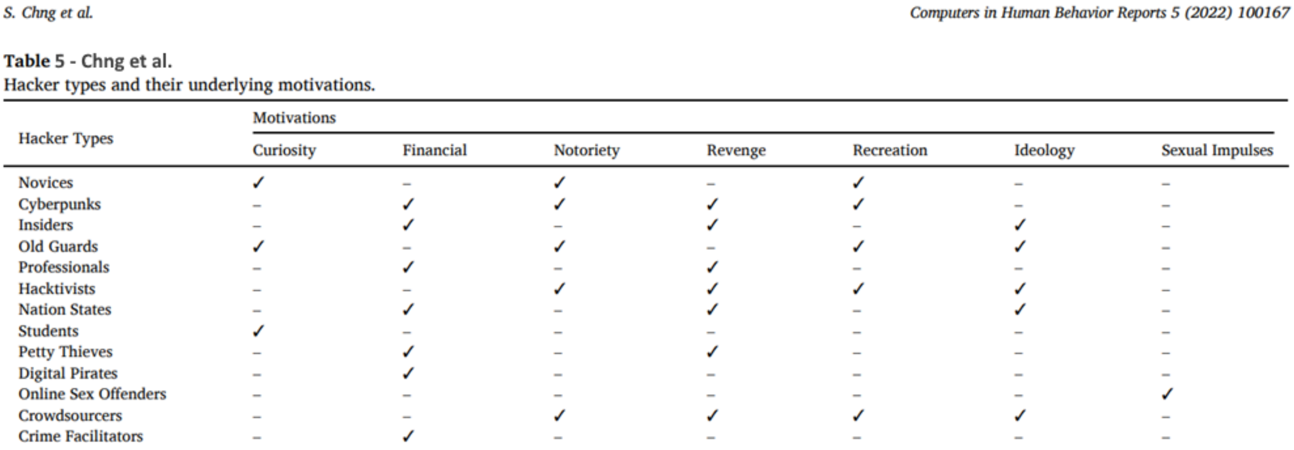
Motives	Ideology, possible cyber warfare
Criminal Intent	High
Resources	High skill levels and funding
Activities	Information monitoring, cyber espionage, leaking, destructive attacks; Spear phishing, zero-day exploits
Level of danger posed	High, significant level of damage and destruction intended
Type of risk posed	Reputational and/or operational risk, indirectly linked to financial

[111] TeamPassword. (2021). Who is Fancy Bear and how can you protect yourself?.

[112] Moeckel. (2019). Examining and Constructing Attacker Categorisations: an Experimental Typology for Digital Banking.

2.4. Chng et al.'s typology

This last framework represents the newest work in the classification of hackers in cyber security studies. Chng et al.'s typology focuses solely on the motivations of the hackers as the distinctive factor, while also describing by word different strategies of the actors. Their work is interesting as they took an approach of synthesizing all the previous typologies and taxonomies to create a new, all-encompassing one, which is based on the updated terminologies used within the cyber community. Their tables are reminded below.[113]



S. Chng et al. *Computers in Human Behavior Reports 5 (2022) 100167*

Table 5 - Chng et al.
Hacker types and their underlying motivations.

Hacker Types	Motivations						
	Curiosity	Financial	Notoriety	Revenge	Recreation	Ideology	Sexual Impulses
Novices	✓	–	✓	–	✓	–	–
Cyberpunks	–	✓	✓	✓	✓	–	–
Insiders	–	✓	–	✓	–	✓	–
Old Guards	✓	–	✓	–	✓	✓	–
Professionals	–	✓	–	✓	–	–	–
Hacktivists	–	–	✓	✓	✓	✓	–
Nation States	–	✓	–	✓	–	✓	–
Students	✓	–	–	–	–	–	–
Petty Thieves	–	✓	–	✓	–	–	–
Digital Pirates	–	✓	–	–	–	–	–
Online Sex Offenders	–	–	–	–	–	–	✓
Crowdsourcers	–	–	✓	✓	✓	✓	–
Crime Facilitators	–	✓	–	–	–	–	–

[114]

[113] Chng et al. (2022). Hacker types, motivations and strategies: A comprehensive framework.

[114] Ibid.

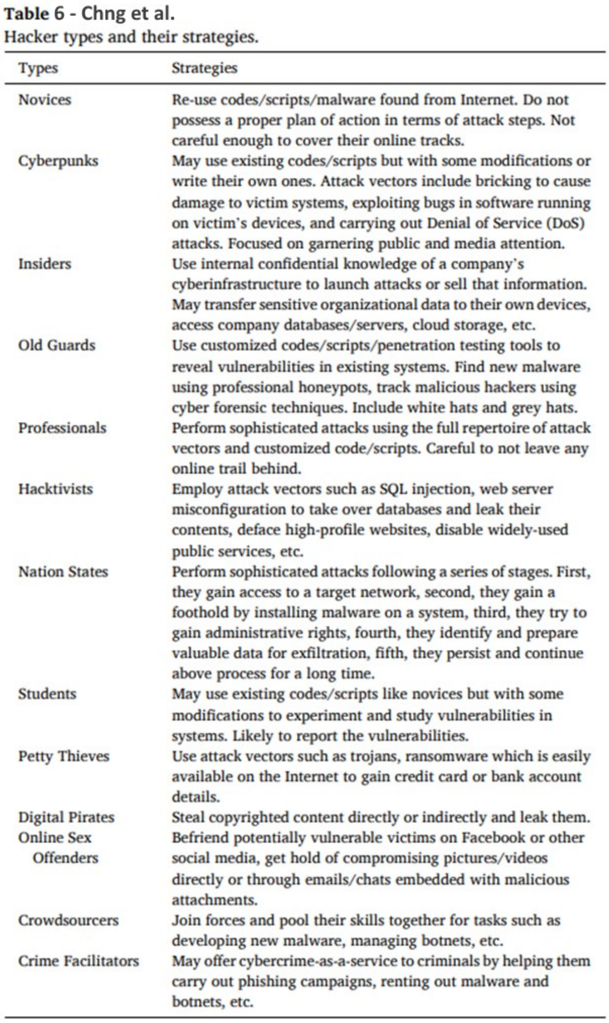


Table 6 - Chng et al.
Hacker types and their strategies.

Types	Strategies
Novices	Re-use codes/scripts/malware found from Internet. Do not possess a proper plan of action in terms of attack steps. Not careful enough to cover their online tracks.
Cyberpunks	May use existing codes/scripts but with some modifications or write their own ones. Attack vectors include bricking to cause damage to victim systems, exploiting bugs in software running on victim's devices, and carrying out Denial of Service (DoS) attacks. Focused on garnering public and media attention.
Insiders	Use internal confidential knowledge of a company's cyberinfrastructure to launch attacks or sell that information. May transfer sensitive organizational data to their own devices, access company databases/servers, cloud storage, etc.
Old Guards	Use customized codes/scripts/penetration testing tools to reveal vulnerabilities in existing systems. Find new malware using professional honeypots, track malicious hackers using cyber forensic techniques. Include white hats and grey hats.
Professionals	Perform sophisticated attacks using the full repertoire of attack vectors and customized code/scripts. Careful to not leave any online trail behind.
Hacktivists	Employ attack vectors such as SQL injection, web server misconfiguration to take over databases and leak their contents, deface high-profile websites, disable widely-used public services, etc.
Nation States	Perform sophisticated attacks following a series of stages. First, they gain access to a target network, second, they gain a foothold by installing malware on a system, third, they try to gain administrative rights, fourth, they identify and prepare valuable data for exfiltration, fifth, they persist and continue above process for a long time.
Students	May use existing codes/scripts like novices but with some modifications to experiment and study vulnerabilities in systems. Likely to report the vulnerabilities.
Petty Thieves	Use attack vectors such as trojans, ransomware which is easily available on the Internet to gain credit card or bank account details.
Digital Pirates	Steal copyrighted content directly or indirectly and leak them.
Online Sex Offenders	Befriend potentially vulnerable victims on Facebook or other social media, get hold of compromising pictures/videos directly or through emails/chats embedded with malicious attachments.
Crowdsourcers	Join forces and pool their skills together for tasks such as developing new malware, managing botnets, etc.
Crime Facilitators	May offer cybercrime-as-a-service to criminals by helping them carry out phishing campaigns, renting out malware and botnets, etc.

[115]

2.4.1. The Shadow Brokers

Based on the analysis of The Shadow Brokers' motivations that was done in part 2.1.1.1., it was concluded that financial gain, ideology, notoriety, and possibly even revenge could be the main motivators of the group. Chng et al. include *curiosity, recreation,* which is described as challenge and thrill-seeking, and *sexual impulses* as the remaining motivations. It can be derived that The Shadow Brokers indeed sought out a challenge since they picked the NSA as their target. Therefore, the *recreation* motivation could be also ticked. This leaves us with every motivation except *curiosity* and *sexual impulses.* As we can see in the table, there is no category fulfilling the same criteria. The closest categories based on their motivations are *Cyberpunks* though they do not tick the ideology box, *Hacktivists* who, however, do not look for financial gain, and

[115] Ibid.

Crowdsourcers who have the same issue. Both *Insiders* and *Nation states*, which were presumed to be the possible identity of The Shadow Brokers do not include *notoriety* and *recreation* in Chng et al.'s table.

Of the closest three categories, the *Crowdsourcers* are ruled out in the strategy section since The Shadow Brokers do not join forces nor pool their skills with anyone. However, both the *Cyberpunks* and the *Hacktivist* descriptions of strategies could fit. The Shadow Brokers focused on public and media attention, as well as they could have exploited a bug in software to gain access to the NSA. They leaked the contents, and from a layman's point of view could have also employed SQL injection, a code injection technique targeting data-driven applications, or could have attacked using server misconfiguration, and exploited configuration weaknesses found in web and application servers. However, there is no information about how they actually accessed the NSA's systems. According to the strategies, however, both *Insiders*, as well as the *Nation States*, fit the most precisely. Nevertheless, Chng et al.'s framework may be the most updated but is far from ideal for the case of The Shadow Brokers.

2.4.2. Fancy Bear

As for the motivations of Fancy Bear, *curiosity,* as well as *financial* and *sexual impulses,* could be excluded right away. Even though Fancy Bears' attacks attract a lot of attention since they mainly leak important data in support of the Russian Federation, the group also often poses as someone else, usually a hacktivist such as Anonymous, to further their case.[116] Therefore, I would also exclude *notoriety* and possibly even *recreation*, even though the group might seek challenge, I suppose other motivators are determining the group's actions. The main one is *ideology.* Again, the *revenge* would make sense with the WADA attack, however, the question of whether ideology was not the main motivator behind the revenge is still too important to include as an independent motivation.

Therefore, all of Chng et al.'s categories are far from being applicable since none of them has only *ideology* as a motivator. If we were to include *revenge* in the equation, then the closest category would be *Insiders,* however, they are also motivated by *financial* gain*,* according to the authors. We presume Fancy Bear to be a state-sponsored APT based on

[116] Cybersecurity Help. (2022). The story of the four bears: Brief analysis of APT groups linked to the Russian government.

empirical data, however, in this typology the *Nation States* are supposed to be motivated by *ideology, revenge,* and again *financial* gains. The motivation, therefore, does not precisely fit none of the categories.

The strategies are on the other hand fitting more categories, both *Nation States* and *Hacktivists* are applicable. However, also *Cyberpunks* and *Professionals* could not be ruled out since Fancy Bear garners public and media attention, and perform sophisticated attacks, although they could do a better job of not leaving any trail behind.

Chng et al.'s categorization is so far the most confusing and least telling one. The separate issues of the category will be discussed in the last section.

2.5. Threat profiling in praxis – Irwin's approach

Finally, there is the dimension of praxis to include in this thesis. This paper is valuable for this thesis as it lets us compare the theory of studying hackers or threat actors to reality. Specifically, to the instructions for organizations on how to proceed in practice. Even though the NSA probably does not need a universal guide on how to protect itself, it was still attacked, so this could potentially benefit from Irwin's work as well. Not to mention all the organizations, industries, and governments that Fancy Bear has targeted over the years. Threat profiling by Irwin is a Global Information Assurance Certification Paper and includes much more than just threat actor categorizations. Nevertheless, they are a vital part of creating specific threat profiles advising incident management for the organizations. Therefore, they can be dissected and subjected to testing for this thesis.

2.5.1. The Shadow Brokers

Irwin firstly calls for a few words of description of each category. A brief description of The Shadow Brokers could sound like this: "Either state-sponsored, or an insider threat with by far only one target of a governmental sort. Seeking primarily financial profit with strong ideological implications and an effort to become notorious." The relationship would depend on the fact whether The Shadow Brokers are the insider, ergo internal relationship, or external in the case of a state-sponsored group. However, Irwin also mentions the relationship of a *partner*, which is an interesting thought that cannot be ruled out either. The region of operation was established as being most probably the United States, with the possibility of Russia. Even according to Irwin's description of these two regions in the *state-sponsored* category, these two would fit. For Russia/Eastern

Europe Irwin states: “These cyber-attacks are more technically advanced and highly effective at evading detection. Russia’s attacks are the most complex and advanced and are stealthier than Chinese attacks. There is more focus on Zero-day exploits.”[117] Whereas the United States is described as: “The United States uses the most complex, targeted, and rigorously engineered cyber-attack campaigns to date. The attacks require a high level of financial investment, technical sophistication, and legal oversight which, all combined, make these attacks stand apart from the others.”[118]

Motive again is *Financial gain* and *Ideological* according to Irwin’s options. The intent would be *Deliberate, Malicious,* and even possibly *Competitive* since the author includes it and The Shadow Brokers’ doing could be regarded as competing with the NSA, at least in a form of bragging. Their *Capability* dimension unquestionably includes high technical capabilities, stealthy, patient, and persistent, and high intensity. The number of attackers, as well as the funding, is not determinable. The Shadow Brokers’ *Target victim* is the public sector and their actions included as far as we know, capturing stored data, possibly spyware or stolen credentials, which are forms of malware and hacking, and maybe even privileged access or using a partner relationship. The category of *Action* is due to a lack of public information difficult to fill out.

Next is the *Targeted Asset,* it is possible that the hackers were able to target the Windows desktops and servers, Unix (Linux & Solaris), and embedded devices such as routers, after they stole material to do so, however, certainly, they targeted various NSA’s trade secrets and intellectual property.[119] And finally, the *Objective* would possibly be exfiltrating data, possibly by abusing access privilege, and information theft, which would include Internal Organizational Data, Trade Secrets, and System Information. The table for The Shadow Brokers would therefore look like Table 14.

Table 14 – The Shadow Brokers according to Irwin	
Name:	The Shadow Brokers
Description: Either state-sponsored or an insider threat with by far only one target of a governmental sort. Seeking primarily financial profit with strong ideological implications and an effort to become notorious.	

[117] Irwin. (2014). Creating a Threat Profile for Your Organization.

[118] Ibid.

[119] Suiche. (2017). The Shadow Brokers Cyber Fear Game-Changers.

Relationship: Internal / External / Partner	**Region of Operation:** United States / Russia
Motive: Financial gain, Ideological	**Intent:** Deliberate, Malicious, Competitive.
Capability: High technical capabilities, stealthy, patient, persistent, and high intensity.	
Target Victim: Public sector: NSA	
Action: Capturing stored data, possibly spyware or stolen credentials (malware and hacking) and maybe even privileged access or using partner relationship.	
Targeted Asset: Trade secrets, Intellectual Property, High-level employees.	
Objective: Data exfiltration (possibly by abusing access privilege) and information theft: Internal Organizational Data, Trade Secrets, System Information.	

According to this table, The Shadow Brokers group is most similar to the *State-Sponsored Threat Actors,* in which case not surprisingly also exists the issue with motivation since it this category is not motivated by *Financial gain.* However otherwise, all dimensions are remarkably close to this category. Secondly, the group also resembles the category of a *Partner.* Where there is an issue of motivation not including ideology and intent not including malicious. Nevertheless, the rest is also very accurate. The classifications are depicted in Table 15 and Table 16.

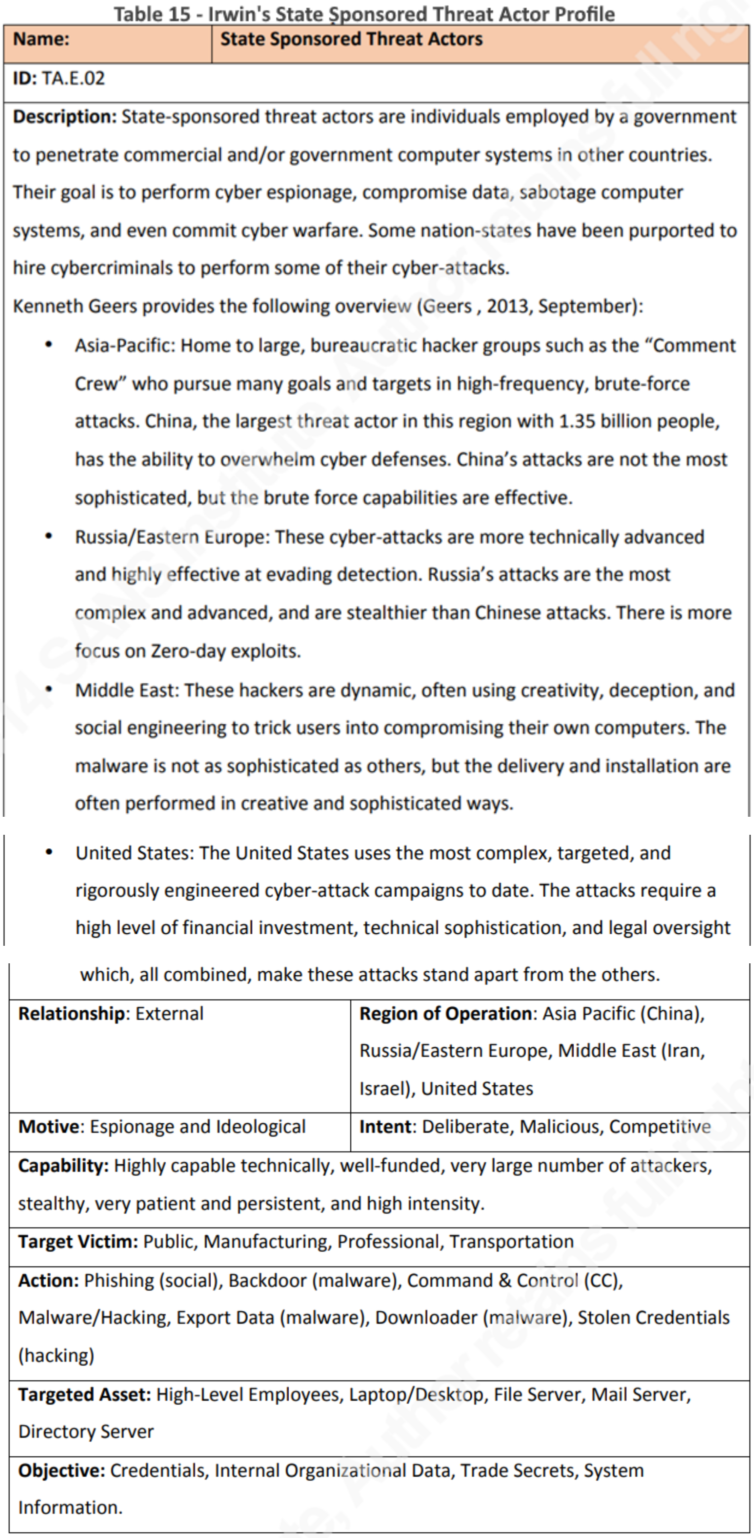


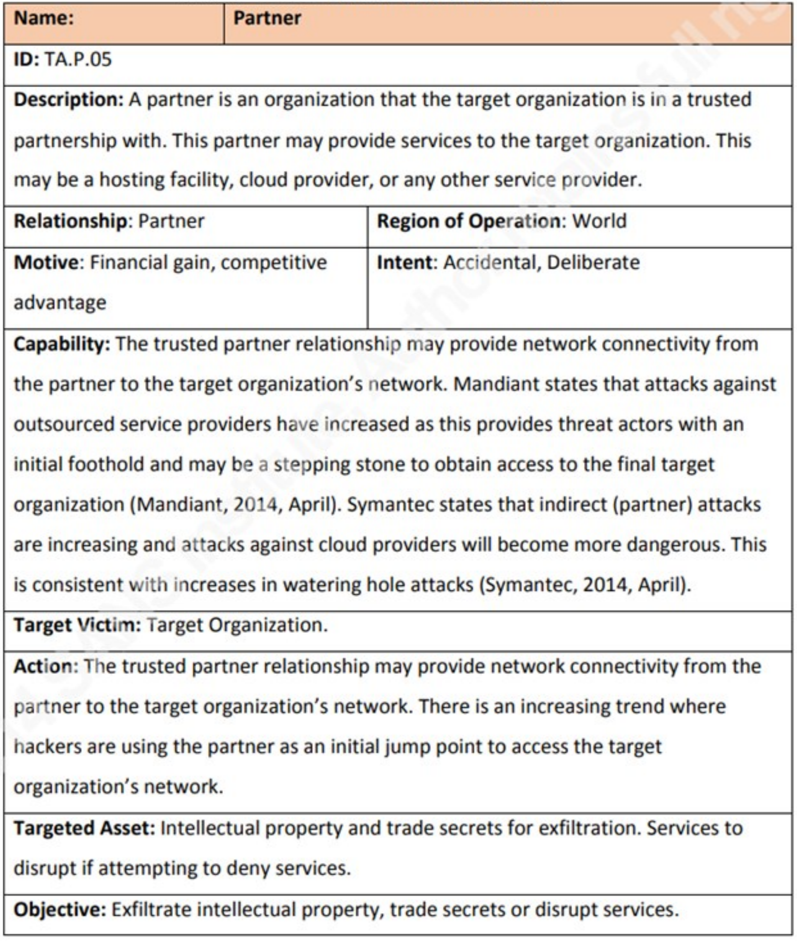
Table 15 - Irwin's State Sponsored Threat Actor Profile

Name:	**State Sponsored Threat Actors**
ID: TA.E.02	
Description: State-sponsored threat actors are individuals employed by a government to penetrate commercial and/or government computer systems in other countries. Their goal is to perform cyber espionage, compromise data, sabotage computer systems, and even commit cyber warfare. Some nation-states have been purported to hire cybercriminals to perform some of their cyber-attacks. Kenneth Geers provides the following overview (Geers , 2013, September): • Asia-Pacific: Home to large, bureaucratic hacker groups such as the "Comment Crew" who pursue many goals and targets in high-frequency, brute-force attacks. China, the largest threat actor in this region with 1.35 billion people, has the ability to overwhelm cyber defenses. China's attacks are not the most sophisticated, but the brute force capabilities are effective. • Russia/Eastern Europe: These cyber-attacks are more technically advanced and highly effective at evading detection. Russia's attacks are the most complex and advanced, and are stealthier than Chinese attacks. There is more focus on Zero-day exploits. • Middle East: These hackers are dynamic, often using creativity, deception, and social engineering to trick users into compromising their own computers. The malware is not as sophisticated as others, but the delivery and installation are often performed in creative and sophisticated ways. • United States: The United States uses the most complex, targeted, and rigorously engineered cyber-attack campaigns to date. The attacks require a high level of financial investment, technical sophistication, and legal oversight which, all combined, make these attacks stand apart from the others.	
Relationship: External	**Region of Operation**: Asia Pacific (China), Russia/Eastern Europe, Middle East (Iran, Israel), United States
Motive: Espionage and Ideological	**Intent**: Deliberate, Malicious, Competitive
Capability: Highly capable technically, well-funded, very large number of attackers, stealthy, very patient and persistent, and high intensity.	
Target Victim: Public, Manufacturing, Professional, Transportation	
Action: Phishing (social), Backdoor (malware), Command & Control (CC), Malware/Hacking, Export Data (malware), Downloader (malware), Stolen Credentials (hacking)	
Targeted Asset: High-Level Employees, Laptop/Desktop, File Server, Mail Server, Directory Server	
Objective: Credentials, Internal Organizational Data, Trade Secrets, System Information.	

[120]

[120] Irwin. (2014). Creating a Threat Profile for Your Organization.

Table 16 - Irwin's Partner Threat Actor Profile



Name:	**Partner**
ID: TA.P.05	
Description: A partner is an organization that the target organization is in a trusted partnership with. This partner may provide services to the target organization. This may be a hosting facility, cloud provider, or any other service provider.	
Relationship: Partner	**Region of Operation**: World
Motive: Financial gain, competitive advantage	**Intent**: Accidental, Deliberate
Capability: The trusted partner relationship may provide network connectivity from the partner to the target organization's network. Mandiant states that attacks against outsourced service providers have increased as this provides threat actors with an initial foothold and may be a stepping stone to obtain access to the final target organization (Mandiant, 2014, April). Symantec states that indirect (partner) attacks are increasing and attacks against cloud providers will become more dangerous. This is consistent with increases in watering hole attacks (Symantec, 2014, April).	
Target Victim: Target Organization.	
Action: The trusted partner relationship may provide network connectivity from the partner to the target organization's network. There is an increasing trend where hackers are using the partner as an initial jump point to access the target organization's network.	
Targeted Asset: Intellectual property and trade secrets for exfiltration. Services to disrupt if attempting to deny services.	
Objective: Exfiltrate intellectual property, trade secrets or disrupt services.	

[121]

For The Shadow Brokers, given that this typology includes a lot of dimensions, it is very accurate, while also providing a new category of threat actor that the previous typologies omitted – the *Partner*, which is also surprisingly fitting for this case.

2.5.2. Fancy Bear

Finally, there is the hacker group Fancy Bear to put to the test. A brief description of the group could sound like this: "Probably a state-sponsored APT with links to Russian GRU's military intelligence agency. Also known as APT28, Pawn Storm, Sofacy Group, Sednit or STRONTIUM. While focusing on cyber espionage and subversion, the group has a peculiar modus operandi since instead of typical industrial espionage, they tend to leak stolen information in support of Russia's political interests." The relationship is logically external, and the region of operation is Russian. Motives would include espionage, ideology, and intent would unquestionably be deliberate, malicious, and competitive.

[121] Ibid.

Capabilities of Fancy Bear could be described as: “Highly capable technically, stealthy, very large number of attackers, well-funded, very patient and persistent, and high intensity.” Targeted Victims could include the Public (mainly governmental institutions), Information (Media), Financial, Energy sector, Military, NGOs and Non-profits, Aerospace[122] and even the pharmaceutical industry, when they targeted pharma and clinical organizations conducting COVID-19 vaccine and treatment research.[123]

Fancy Bear’s actions include as already mentioned mainly spear-phishing, and regular phishing emails, they steal credentials, exploit zero-day vulnerabilities, utilize backdoors[124] and altogether both malware and hacking techniques. The main targeted asset of this group were high-level employees such as governmental representatives, and mainly mail servers as in the 2016’s U.S. elections hack and many other instances.[125] And finally, the objective could include all of Irwin’s possibilities, which are Credentials, Internal Organizational Data, Trade Secrets, and System Information.[126] In Irwin’s form of visualization, the case of Fancy Bear would look like Table 17.

Table 17 – Fancy Bear according to Irwin

Name:	Fancy Bear
Description: Probably a state-sponsored APT with links to Russian GRU’s military intelligence agency. Also known as APT28, Pawn Storm, Sofacy Group, Sednit or STRONTIUM. While focusing on cyber espionage and subversion, the group has a peculiar modus operandi since instead of typical industrial espionage, they tend to leak stolen information in support of Russia’s political interests	
Relationship: External	**Region of Operation:** Russia
Motive: Espionage and Ideological.	**Intent:** Deliberate, Malicious, Competitive.

[122] Crowdstrike. Fancy Bear.

[123] Seals, T. (2020). Nation-State Attackers Actively Target COVID-19 Vaccine-Makers. *Threat post.* https://threatpost.com/russia-north-korea-attacking-covid-19-vaccine-makers/161205/.

[124] Osborne, Ch. (2019). Political targets at risk as Fancy Bear returns with refreshed backdoor malware. *ZDNet.* https://www.zdnet.com/article/political-targets-at-risk-as-fancy-bear-returns-with-refreshed-backdoor-malware/.

[125] TeamPassword. (2021). Who is Fancy Bear and how can you protect yourself?.

[126] Lyngaas, S. (2020). When Fancy Bear isn’t so Fancy: APT group’s ‘crude’ methods continue to work. *CyberScoop.* https://www.cyberscoop.com/fancy-bear-trend-micro-russia-espionage/.

Capability: Highly capable technically, stealthy, very large number of attackers, well-funded, very patient, and persistent, and high intensity.
Target Victim: Public (mainly governmental institutions), Information (Media), Financial, Energy sector, Military, NGOs and Non-profits, Aerospace, Pharmaceutical industry.
Action: Spear-phishing, Phishing, Zero-day exploits, Backdoor, Malware/Hacking, Stolen Credentials.
Targeted Asset: Mainly High-Level Employees and Mail Servers.
Objective: Credentials, Internal Organizational Data, Trade Secrets, and System Information

If we were to compare this table to the *State-Sponsored Threat Actors,* they are, other than the negligible differences between the targeted victims of the group, identical, representing the first classification that is highly accurate with the case of Fancy Bear.

3. Results of testing

In this section, findings from the tests of cross-disciplinary frameworks are explained with a specific focus on their shortcomings. Firstly, the specific models are discussed followed by the disciplinary comparative part. This part also answers the first research question: What are the issues and virtues of tested typologies and models?

3.1. Social studies results

None of the hacker groups did precisely fit into Seebruck's taxonomy. Though they can be visualized by the updated weighted arc circumplex model, there is still an issue with the categorization. Although an exception could be made here with The Shadow Brokers, to classify them as *Insiders* since the organization they would be an insider of, employs very experienced and skilled hackers. A lot of empirical evidence also points to the hacker(s) being an insider. Nevertheless, The Shadow Brokers' motivations would still not align even with the properties of this category. Here, the biggest issue with The Shadow Brokers seems to be the difference between being motivated by revenge and being motivated by ideology. *Ideology* is described as "political activists (those motivated by contemporary social issues) as well as nationalists (attacks initiated by patriotic civilians or state-sponsored cyber warfare)" while *Revenge* as "both personal vengeance (e.g. inside jobs by disgruntled workers) and larger social justice issues (e.g. online crowdsourcing movements)".[127] However, as I described earlier, after primary profit, ideology, not revenge, is most probably the secondary motivation for the group, unlike Seebruck's insider.

Furthermore, if the group should be put in the *cyber warrior* category*,* the prestige is missing, and the order of ideology and profit is questionable.

Both groups should be, based on their skill level, classified as *cyber warriors.* However, even if The Shadow Brokers would be a specific case that could count as an exception from Seebruck's taxonomy, Fancy Bear's motives were also not correct. Even though some state-sponsored APTs go after a financial profit (f.e. the North Korean ones), it is still an exceedingly small part of the whole. Usually, APTs are stealing data, even from financial institutions, mainly for political gain.[128] It is important to point out, however, the advantage of Seebruck's framework, which is the weighted arc circumplex model since it is capable of depicting multiple motivations by their intensity.

It seems like the case of The Shadow Brokers would fit more into the previous models from social scientists if it were a case of nation-state hackers although all of them lack the notoriety motivation that The Shadow Brokers have. Since their models do not include ideology as a separate motivator, it could be assumed that revenge encompasses this issue. Roger's *Information warriors* are depicted in the quadrant showing financial motivation, very close to revenge. Meyers et al.'s *Cyber terrorists* are motivated primarily by profit and secondarily by revenge. As well as Hald and Pedersen's *Nation States* category is motivated half by financial gain and half by revenge.

If The Shadow Brokers were a case of insiders, both Meyers et al.'s and Hald and Pedersen's typologies which include this category, place them inside the revenge quadrant fairly close to financial motivation. The notoriety, however, is also lacking and the group should find themselves in the profit quadrat.

Furthermore, if we were to compare the Fancy Bear to the previous models from the field of social sciences, they do not align with this type of threat actor as well as in

[127] Seebruck. (2015). A typology of hackers: Classifying cyber malfeasance using a weighted arc circumplex model.

[128] Loffredo, M. (2020). U.S. Cyber Intelligence Warning Highlights Security Threat From Nation-Sponsored Advanced Persistent Threats (APTs) – Part 1. *The Firewall.* Retrieved from: https://www.thefirewall-blog.com/2020/06/u-s-cyber-intelligence-warning-highlights-security-threat-from-nation-sponsored-advanced-persistent-threats-apts-part-1/.

Seebruck's case. Roger's *Information warriors* are said to be motivated by patriotism, however, in the circumplex model, they are depicted in a financial motivation quadrant, closely to revenge. In Meyers et al.'s *Cyber terrorist* category, the authors explain their motivation as ideology, politics, and espionage, yet in the model, it is again depicted in the financial quadrant close to revenge. And finally, in Hald and Pederson's model, the *Nation States* find themselves right in the middle of the two quadrants. It could be deducted, therefore, that the older typologies from the field of social sciences are more accurate in this case, however, their models are not matching the accuracy. Seebruck's weighted arc model, even if not precisely fitting by the motivations, is at least more aligned with his proposed typology.

The conclusion for this section is that the category of *Insider,* which should be applicable for The Shadow Brokers, is almost entirely wrong. The prestige motivation is missing in both options The Shadow Brokers could fit in and profit is redundant with Fancy Bear. However, the weighted arc model is still the best in the whole discipline since it depicts more than two motivations at once as well as their intensity. Based on the cases, the typology is, therefore, fairly wrong, the model, however, is a great asset.

Finally, if I were to suggest updates for Seebruck's typology that would make the cases fit, it would firstly concern the category of *Insider*. The Shadow Brokers could be an insider based on empirical data, but the category does not include ideology as a motivation. Therefore, I would include it in the typology since it is not only a case of The Shadow Brokers but also fits other examples such as the case of Snowden. I would also add a disclaimer to this category that the skills of the Insider should depend on the organization they come from. Secondly, I would change the profit motivation of *Cyber warriors* by either discarding completely or making it less important. Financial motivation does not work with Fancy Bear nor with most other state-sponsored APTs nowadays. What Seebruck's work also lacks is a proper description of the categories. Although partly excusable since he aims at updating the model based on Roger's and Meyers et al.'s typologies, if his update was to be properly usable, he should also include at least a brief description of each hacker category.

3.2. Results from the field of cyber security

3.2.1. de Bruijne et. al. results

In de Bruijne et al.'s typology, The Shadow Brokers have again a motivation issue, would they be a case of state actors and state-sponsored networks. The *insider* category was, however, highly accurate, although this typology has an issue with defining one dimension, the level of resources. The authors state that the resources are high if there was an unnoticed breach for a long time before the actual attack, or in a figurative sense with the case of The Shadow Brokers before they leaked the stolen information. On the other hand, they also state that an *insider* has a low level of resources since it is only one person. The problem arises when both the eventualities exist at the same time as was the case of The Shadow Brokers. How high are the resources if there is only one individual, but he/she managed to stay unnoticed by the attacked organization for a long time?

If the group was not an insider, there is another issue with the remaining categories. Both *state-sponsored networks* and *state actors* are, according to the authors, motivated only by geopolitical interests, which is most probably not true with The Shadow Brokers. The Fancy Bear group also shows another issue with these two categories. That is that citizens are lacking as a target with both. Furthermore, the state-sponsored APTs are very sophisticated groups, making it considerably difficult to trace them and attribute their crimes. Therefore, it is questionable whether the differentiation between the *state-sponsored networks* and *state actors* is necessary since there is usually very little information about the organizational grouping of the threat actor.

De Bruijne et al.'s typology has on the other hand also advantages. Firstly, it encompasses more dimensions in the categorizations and not just motivation. Specifically, it has five main dimensions with at least three subcategories each. Considering this, it is surprisingly accurate. The case of insider is, except for the questionable resources, highly fitting with The Shadow Brokers as well as both categories for Fancy Bear.

If I were to propose an update for this typology, it would be to clarify the issue of resources for the *insider* category and possibly merge the *state-sponsored networks* and *state actors* categories since the only difference between them is a form of organization, which is often a very difficult aspect to prove. Other than that, de Bruijne et al.'s typology is highly accurate in both tested cases.

3.2.2. Moeckel's results

In the case of The Shadow Brokers, there is a surprising result with Moeckel. The *officials* were discarded as a possible category for the group since there were too many differences. However, the *insider* category, which was in the previous tests one of the most fitting, is with Moeckel's typology in the second place after a new category – *ideologists.* The reason behind that is that the *insider* is missing ideology as one of the motivations, the activities are not very fitting, and the reputational type of risk is with this category the least probable. The *ideologists* on the other hand have only one issue and that is the relatively insufficiently descriptive definition of the activities dimension, where it only says: "social and political background to attacks"[129] unlike the other categories where the activities are described in greater detail.

Nevertheless, there is one important virtue of Moeckel's framework. The concept of third-party supplier is introduced with the category of *insider*. It is the first work that considers the possibility that the attacker would be a partner to the targeted organization, which could be the case of The Shadow Brokers.

As for Fancy Bear, Moeckel presents the possibility of them being cyber terrorists since it is one of the representatives of the *ideologists* category, which the group identically imitates. The second most probable category for Fancy Bear is the *officials,* however, Moeckel states that they like to stay undetected, and it is known of this particular group to not be so cautious in covering their tracks, which is rather abnormal for a state-sponsored actor.

It is strange that according to Moeckel, both The Shadow Brokers and Fancy Bear would fall into the same category because the groups behave very differently in reality. Although the cases could be fitted rather easily into Moeckel's categories, the *insider* category is similarly to Seebruck's missing the ideology motivation and the reputational type of risk is with this category the least probable, which differs from the case of The Shadow Brokers.

In conclusion, Moeckel's framework is highly accurate by theory, which is admirable since there are 6 dimensions to classify hacker groups by. The accuracy, however, becomes problematic, when the reality of the differences between both the

[129] Moeckel. (2019). Examining and Constructing Attacker Categorisations: an Experimental Typology for Digital Banking.

groups is considered. Nevertheless, the only minor update I would propose for this typology would be to specify the activities of *ideologists* since a social or political background is not a form of activity compared to what Moeckel describes with the other categories.

3.2.3. Chng et al.'s results

Chng et al.'s framework updated the previous typologies. However, it only includes motivations and strategies, which are described in a word. For The Shadow Brokers, the categories of *cyberpunks, and hacktivists* are the most similar according to their motivations as well as strategies, however, they all miss one of the main motivations of The Shadow Brokers. On the other hand, according to strategies, the hackers would fit better both the *nation states* and *insiders* but as mentioned the motivations according to the authors are not compatible with this case.

The case of Fancy Bear is similarly wrong, the most fitting category according to their motivations is *insiders*, which is impossible according to empirical evidence. The strategies are most similar to the *nation states* and *hacktivists*, however, these categories are not aligned with the group's motivations.

By far, Chng et al.'s framework is the least accurate. The reason behind that might be the lack of dimensions which are used for classification. Even though there is the biggest number of motivators so far, it is apparent that this dimension is not enough even with the combination of descriptions of strategies. The only advantage of this typology is that the ideological motivation is finally mentioned for the first time in the category of the *insider*, which was lacking in the case of The Shadow Brokers with the previous typologies.

I do not propose an update for Chng et al.'s framework since based on the tests it is almost entirely wrong.

Conclusion of cyber security hacker classifications

In conclusion, the most accurate typology from the field of cyber security hacker research based on the testing in this thesis is de Bruijne et al.'s, which is a framework that included target, expertise, resources, type of organization, and motivation as its dimensions. The worst one, on the other hand, is Chng et al.'s, showing that a small number of dimensions used for classifications of the hacker group, in this case motivation, and a brief description of strategies, is a cause for unreliability and failure of typology.

It is however interesting, that even if the typologies have their issues, together they indicate that the real identity of The Shadow Brokers, could actually be a case of an insider based on the comparison of empirical data and the dimensions created by researchers. The Fancy Bear not surprisingly is indicated to be an official or state-sponsored APT.

3.3. Results of profiling in praxis

Irwin wrote his paper in 2014, therefore, in the time before cyber security experts conducted proper research on hacker classifications. He includes a lot of practical information concerning the whole concept of threat profiling and organizational safety. The greatest virtue is, in my opinion, the single-standing category of a *partner*. The Shadow Brokers fitted quite nicely into this category, taking into account the ten dimensions, so far, the biggest number, the author considers. The group also fitted into the *state-sponsored threat actors* category, though a financial motivation is missing, which as debated in the thesis, should not be included in this category, however, it is for The Shadow Brokers still of a slightly better fit than *partner* one. The *partner* had specifically three issues, which are also connected to the update I would like to propose. Firstly, the only motivations Irwin recognizes are espionage, competitive advantage, ideology, and financial gain. Completely discarding the notions of a hacker being motivated by curiosity, striving for notoriety, or seeking revenge. The *partner* category itself would, in my opinion, benefit from including revenge, together with ideology to its motivations. With that in mind, I would also include malicious intentions as a possibility for this type of threat actor since it is likely that The Shadow Brokers were a partner of the NSA, and their intent was definitely malicious. Finally, the description of capabilities in this category is rather confusing compared to other threat actors, which follow the same descriptive pattern. For uniting the whole framework, I would propose using the same wording in this section.

As for Fancy Bear, Irwin's framework was almost completely accurate. The only issue was with the targeted section, which I would propose could include more types of targets than just public, manufacturing, professional, and transportation, which the author includes in the *state-sponsored threat actors* typology. Other than that, it was correct, surprisingly with regards to the time, Irwin's work was written.

The last update I would propose for this framework would be to merge or, on the contrary, to better differentiate between the dimensions of the targeted asset and objective since these two are mostly identical and cause the issue of redundancy in otherwise comprehensible classification.

3.4. Cross-disciplinary comparison of the classifications

Finally, this part answers the research questions of the similarities of tested typologies and models, if the frameworks are applicable for the novel types of threat actors, and what specific factors have proven to be most important after testing. It is aiming to do so by comparing the approaches to the classifications of the disciplines.

Firstly, none of the disciplines had a precise category for the case of The Shadow Brokers. However, the cyber security researchers have made updates on the category of *insiders* and included ideology as one of the motivators, which was missing in the previous works. Moreover, they have introduced more dimensions to classify the hacker groups by, which could potentially mean a greater possibility of deviation of categories from real cases, however, that was not the case here. In fact, the opposite happened, and they have managed to do a better job of creating a classification where The Shadow Brokers fitted more precisely. One research has even introduced a possibility of a *partner* as a malicious threat actor, which confirmed a high probability for The Shadow Brokers by the empirical data. The notion of the partner was, however, best elaborated on in Irwin's paper, which was supposed to represent the field of cyber security in practice and was written already in 2014, preceding the cyber security researchers.

Irwin was also the first one to exclude financial motivation from the state-sponsored actors' category, which was a significant issue with the research from social scientists. The cyber security academics have in the majority also adapted this approach (except for Chng et al.) making the case of Fancy Bear fit their classifications better.

The discipline of social science had, however, one big advantage over the other ones. It was the ideas Seebruck proposed, which were later built upon by others. Firstly, it was the notion that hackers are motivated not only by one or two motivations but there is a possibility of a greater number. Secondly, and more importantly, he also introduced a model that was able to depict the intensity of these motivations, which none of the following researchers was able to capture. This aspect could be conceivably useful in practice when the organisations are trying to classify a threat actor by their behaviour to decide which actions are best to respond with.

In general, motivation is the underlying dimension in all the tested frameworks with *financial* and *ideological* appearing in all five. The second place of motivations holds *revenge/retaliation* in all works except Irwin's, and the fourth place is shared by *prestige/notoriety* and *recreation*, which appeared in three out of five papers. Only two were distinguished *curiosity* and *geo-political/espionage*. *Curiosity* appeared less probably for the reason that it is tightly connected to *recreation*, however, if we were to merge these, it would still appear in only three out of five studies. *Geo-political/espionage* was included less perhaps due to its close connection to *ideology*, however, as was shown in the case of The Shadow Brokers, it would be better if these two would be regarded as separate motivators since ideology could be one of the main motivators if the group were a case of a partner or an insider.

There were also proposed some unique types of motivations, mostly in Moeckel's case, who was the only one to include *cause*, *cyber warfare*, and *"making ends meet"*. However, both *cause* and *cyber warfare* were always connected to ideology, therefore a question of redundancy arises. And *"making ends meet"* is also questionable since Moeckel also uses *resources* as a separate category, which would include the fact that the attacker does not have a lot of money. Another unique motivation was the *competitive advantage* in Irwin's case, which in practice could be an important aspect to investigate when preparing a risk management strategy. And lastly, there were *sexual impulses* in Chng et al.'s framework, however, it is debatable whether to include the type of threat actor motivated by *sexual impulses* amongst the others in the categorizations since it is an extremely specific and distinct case.

The second dimension the hacker groups were most classified by is the level of skills. Beginning with the social scientists as the second and last factor, it developed with cyber security research as well as proved to be important in practice with four out of five tested frameworks using it. Chng. et al. are the only ones who decided to omit it. Other authors distinguished in low, medium or high skill levels while some expanded on the notion of skills as sophistication introduced by Seebruck and created a dimension for resources or capabilities which included the money available to the threat actor as well as a number of people, the overall access to the resources, and possibly even political support stealth, persistence, technical strength, intensity, and access to target available to the hackers.

The third most researched dimension was activities, included in three out of five tested works describing the specific technical methods and tools the attacker performed and utilized in the attack. Surprisingly, only two authors considered the target – Irwin, who considered the targeted victim and the targeted asset, and de Bruijne et al., who differentiated between citizens, enterprises, the public sector, and the critical infrastructure as possible targets.

Finally, the exceptions that were considered only once, included type of organization (de Bruijne et al.), the level of criminal intent (Moeckel), type of intent, relationship to the attacked organization, region of operation (all Irwin), level of danger posed (Moeckel), and type of risk posed to the attacked organization (also Moeckel). Irwin was also the only one who included a brief description of the threat actors in the actual table used for the threat profiling, the others sometimes omitted the descriptions at all, or wrote a few words about them in their study but not included them in their visualisations.

Conclusions and propositions

This thesis has proven that both in research and in practice it is vitally important to know why something is happening. Motivation was the underlying factor in all the tested frameworks while skills or sophistication was the second most important dimension. Furthermore, the tested typologies were carefully picked to represent each discipline to allow the comparison of different approaches to studying hacker groups. The thesis shows that there is still no unified typology that would help in research and practice. The case studies of The Shadow Brokers and Fancy Bear have proven that this field of research needs updating at least at the same rate as new threats evolve. One of the greatest issues was finding the correct motivation for The Shadow Brokers. My assumption that it is primary financial could be disputed by some. Nevertheless, when researching a hacker group, there are instances where there is not much information available about it, therefore, one often must guess. The categorizations could supposedly fill in the blanks. However, to be able to do that, they need to be perfected according to the state of the art of threat actor industry. Based on the tests in this thesis I would briefly like to propose a framework that could be beneficial for the field of researching hackers and hacker groups while also answering the last research question: What would the proposed updated dimensions in threat actor typology look like?

Proposed dimensions for a new typology

In this typology, I would include motivations with subcategories of profit, ideology, prestige, revenge, recreation, geo-political, and competitive advantage. The second dimension would be sophistication, including subcategories of the level of skills, and resources available to the group including size, stealth, persistence, and funds, if this data were obtainable. Thirdly, I believe that the targeted victims and assets are equally important as the activities performed by the hackers to breach those targets. The other dimensions that could be included would focus on the level of criminal intent as well as a level of danger posed since those might be different. And finally, I believe the relationship with the victim and if possible whether the intent was deliberate or accidental, are also important aspects to consider. I would propose this typology to be tested in future works since it encompasses all factors which have proven to be important when testing newer sophisticated threats such as The Shadow Brokers, or supposedly state-sponsored APTs such as Fancy Bear.

Summary

The Master's Thesis named "Testing the applicability of hacker typologies and models: A comparative case study of Fancy Bear and The Shadow Brokers" started with the introduction of a conceptual/theoretical framework of the way hacker groups were and are studied in the field of social sciences, and theoretical and practical cyber security. In this framework, different typologies and models were introduced and various categorization techniques were explained. After this step, samples from the three disciplines were picked to be submitted to testing via two hacker groups – The Shadow Brokers and Fancy Bear. Both hacker groups represented a novel type of threat actor while also being distinct enough to provide a greater set of results. The results of the testing were then utilized to analyse the applicability of typologies and models and compare the disciplines. Firstly, the motivation of the hackers represented the underlying factor in all the tested frameworks while skills or sophistication was the second most important dimension. Secondly, the thesis has proven that there is no united approach to researching hacker groups and the existing typologies and models all encompass various issues that need to be dealt with. Thirdly, based on the analysed results of virtues and shortcomings, dimensions for a new typology were proposed. These dimensions would encompass enough criteria to categorize a novel type of actor such as Fancy Bear and The Shadow Brokers. This thesis, therefore, attempts to serve as a stepping stone for creating a new typology, that would be able to embrace the rapid pace at which new threats are evolving. The proposed dimensions of hacker categorizations are now available for further research that could benefit both the field of social sciences as well as cyber security, thereby helping to elevate security studies as a whole.

List of References

Arjen, B., McConnell, A. (2007). Preparing for critical infrastructure breakdowns: the limits of crisis management and the need for resilience. *J Conting Crisis Manag, 15*(1), 50-59. https://onlinelibrary.wiley.com/doi/10.1111/j.1468-5973.2007.00504.x

Associated Press. (2017). Russian hackers hunted journalists in years-long campaign. *Star Advertiser.* https://www.staradvertiser.com/2017/12/22/breaking-news/russian-hackers-hunted-journalists-in-years-long-campaign/.

Atkinson, S. (2019). Psychology and the hacker – Psychological Incident Handling. *SANS Institute.* https://www.scribd.com/document/461604555/psychology-hacker-psychological-incident-handling-36077.

Chng, S., Lu, Y. H., Kumar, A., Yau, D. (2022). Hacker types, motivations and strategies: A comprehensive framework. *Computers in Human Behaviour Reports.* https://www.sciencedirect.com/science/article/pii/S245195882200001X.

Cox, J. (2016). Former NSA Staffers: Rogue Insider Could Be Behind NSA Data Dump. *Vice*. https://www.vice.com/en/article/ezp5na/former-nsa-staffers-rogue-insider-shadow-brokers-theory.

Crowdstrike. *Fancy Bear*. Crowdstrike. https://adversary.crowdstrike.com/en-US/adversary/fancy-bear/.

Cybersecurity Help. (2022). *The story of the four bears: Brief analysis of APT groups linked to the Russian government.* Cybersecurity Help. https://www.cybersecurity-help.cz/blog/2507.html.

Darknet Diaries podcast. *EP 53: SHADOW BROKERS.* Darknet Diaries. https://darknetdiaries.com/transcript/53/.

de Bruijne, M., van Eeten, M., Gañán, C.H. (2017). Towards a new cyber threat actor typology A hybrid method for the NCSC cyber security assessment. *Delft University of Technology - Faculty of Technology, Policy and Management.* https://repository.wodc.nl/handle/20.500.12832/2299.

Donalds, Ch. Osei-Bryson, K-M. (2014). A Cybercrime Taxonomy: Case of the Jamaican Jurisdiction. *CONF-IRM 2014 Proceesings 5.*

http://aisel.aisnet.org/confirm2014/5?utm_source=aisel.aisnet.org%2Fconfirm2014%2F5&utm_medium=PDF&utm_campaign=PDFCoverPages.

Editorial Team. (2019). *Who is Fancy Bear (APT28)?.* Crowdstrike. https://www.crowdstrike.com/blog/who-is-fancy-bear/.

Franceschi-Bicchierai, L. (2016). The NSA Data Leakers Might Be Faking Their Awful English To Deceive Us. *Vice*. https://www.vice.com/en/article/gv5d93/the-shadow-brokers-nsa-leakers-linguistic-analysis.

Furnell, S. (2003). *Cybercrime: Vandalizing the Information Society*. Addison-Wesley. https://link.springer.com/content/pdf/10.1007%2F3-540-45068-8_2.pdf.

Gevirtz Morris. (2019, February 22). *The History of the Word "Hacker".* Deepgram. https://deepgram.com/blog/the-history-of-the-word-hacker-2/.

Gilbert, D. (2015). Equation Group: Meet the NSA 'gods of cyber espionage'. *International Business Times.* https://www.ibtimes.co.uk/equation-group-meet-nsa-gods-cyber-espionage-1488327.

Greenberg, A. (2013). *This Machine Kills Secrets: Julian Assange, the Cypherpunks, and Their Fight to Empower Whistleblowers.* Plume.

Hald, S. LN., Pedersen, J. M. (2012). An Updated Taxonomy for Characterizing Hackers According to Their Threat Properties. In *14th International Conference on Advanced Communication Technology (ICACT)*, 81-86. *IEEE*. https://ieeexplore.ieee.org/document/6174615.

Hannemyr, G. (1997). *Hacking considered constructive*. Oksnoen Symposium on Pleasure and Technology. http://home.sn.no/home/gisle/ oks97.html.

iDnes. (2019). Kyberútok na českou diplomacii způsobil cizí stát, potvrdil Senátu NÚKIB. *iDnes.* https://www.idnes.cz/zpravy/domaci/kyberutok-ceska-diplomacie.A190813_141319_domaci_vlc.

Irwin, S. (2014). Creating a Threat Profile for Your Organization. *Global Information Assurance Certification Paper.* https://www.giac.org/paper/gcih/1772/creating-threat-profile-organization/110995.

Landreth, B. (1985). *Out of the inner circle: a hacker's guide to computer security*. Microsoft Press.

Loffredo, M. (2020). U.S. Cyber Intelligence Warning Highlights Security Threat From Nation-Sponsored Advanced Persistent Threats (APTs) – Part 1. *The Firewall.* Retrieved from: https://www.thefirewall-blog.com/2020/06/u-s-cyber-intelligence-warning-highlights-security-threat-from-nation-sponsored-advanced-persistent-threats-apts-part-1/.

Mass Effect Wiki. *Shadow Broker*. https://masseffect.fandom.com/wiki/Shadow_Broker.

Meyers, C., Powers, S., Fassiol D. (2009). Taxonomies of Cyber Adversaries and Attacks: A Survey of Incidents and Approaches. *Lawrence Livermore National Laboratory*. https://www.osti.gov/biblio/967712/.

Moeckel, C. (2019). Examining and Constructing Attacker Categorisations: an Experimental Typology for Digital Banking. *Proceedings of the 14th International Conference on Availability, Reliability and Security (ARES '19) 93*, 1–6. https://dl.acm.org/doi/pdf/10.1145/3339252.3340341.

Morse, D. and Jackman, T. (2019). NSA contractor sentenced to nine years in theft of massive amounts of classified material. *The Washington Post*. https://www.washingtonpost.com/local/public-safety/nsa-contractor-who-stole-massive-amounts-of-classified-material-set-for-sentencing-friday/2019/07/18/83f1bf96-a995-11e9-9214-246e594de5d5_story.html.

Osborne, Ch. (2019). Political targets at risk as Fancy Bear returns with refreshed backdoor malware. *ZDNet.* https://www.zdnet.com/article/political-targets-at-risk-as-fancy-bear-returns-with-refreshed-backdoor-malware/.

Paganini, P. (2015). The Equation Group shows most complex and sophisticated hacking techniques ever seen. *Security Affairs.* https://securityaffairs.co/wordpress/33637/cyber-crime/the-equation-group-atp.html.

Palenik, L. (2015). *Russian hacking group APT28 planned attacks against global banks*. We live security. https://www.welivesecurity.com/2015/05/14/russian-hacking-group-apt28-planned-attacks-global-banks/.

Rogers, M. K.. (2006). A two-dimensional circumplex approach to the development of a hacker taxonomy. *Digital Investigation 3,* 97–102. https://reader.elsevier.com/reader/sd/pii/S1742287606000260?token=68D1DEE0D78E4F90219BF4B7AE691EBF9B368EF88ACF87E35E4ED98C9622CA1C042025C44FCA26E7A065719E6C38D094&originRegion=eu-west-1&originCreation=20220326154410.

Schneier, B. (2017). Who Are the Shadow Brokers?. *The Atlantic.* https://www.theatlantic.com/technology/archive/2017/05/shadow-brokers/527778/.

Seals, T. (2020). Nation-State Attackers Actively Target COVID-19 Vaccine-Makers. *Threat post.* https://threatpost.com/russia-north-korea-attacking-covid-19-vaccine-makers/161205/.

Secjuice. (2018). *Remember Fancy Bear?.* Secjuice. https://www.secjuice.com/fancy-bear-review/.

Seebruck, R. (2015). A typology of hackers: Classifying cyber malfeasance using a weighted arc circumplex model. *Digital Investigation,* 14, 36-45. https://www.sciencedirect.com/science/article/abs/pii/S1742287615000833

Suiche, M. (2016). Shadow Brokers: The insider theory. *Medium*. https://medium.com/comae/shadowbrokers-the-insider-theory-ded733b39a55#.br7pbm7ar.

Suiche, M. (2017). *The Shadow Brokers Cyber Fear Game-Changers.* Comae technologies. https://archive.org/details/us-17-Suiche-TheShadowBrokers-Cyber-Fear-Game-Changers-wp.

Taylor, Paul A. (1999). *Hackers*. Taylor & Francis Ltd / Books. https://search.ebscohost.com/login.aspx?direct=true&db=sih&AN=18059913&lang=cs&site=ehost-live.

TeamPassword. (2021). *Who is Fancy Bear and how can you protect yourself?.* TeamPassword. https://teampassword.com/blog/who-is-fancy-bear-and-how-can-you-protect-yourself.

The Shadow Brokers. (2016). *Message#1*. Steemit. https://swithak.github.io/SH20TAATSB18/Archive/Messages/TSB/Message1/

The Shadow Brokers. (2016). *Message#5*. Steemit. https://swithak.github.io/SH20TAATSB18/Archive/Messages/TSB/Message5/

The Shadow Brokers. (2017). *Message#10*. Steemit. https://swithak.github.io/SH20TAATSB18/Archive/Messages/TSB/Message10/.

The Shadow Brokers. (2017). *Message#8*. Steemit. https://swithak.github.io/SH20TAATSB18/Archive/Messages/TSB/Message8/.

The Shadow Brokers. (2017). *Message#9*. Steemit. https://swithak.github.io/SH20TAATSB18/Archive/Messages/TSB/Message9/.

The Shadow Brokers' Steemit Messages archive. https://swithak.github.io/SH20TAATSB18/Archive/Messages/TSB/TheShadowBrokers-SteemitMessages/.

Valentová, A. (2021). Decisions Behind the Biggest Leaks in History: What Motivates a Leaker?. *Security Outlines.* Retrieved from: https://www.securityoutlines.cz/the-prototypical-leaker/.

Valentová, A. (2022). Unveiling the Mystery Behind One of the Most Sophisticated Hacker Groups: Who are The Shadow Brokers?. *Security Outlines*. https://www.securityoutlines.cz/unveiling-the-mystery-behind-one-of-the-most-sophisticated-hacker-groups-who-are-the-shadow-brokers/.

WADA. (2016). *Cyber Security Update: WADA's Incident Response*. WADA. https://www.wada-ama.org/en/news/cyber-security-update-wadas-incident-response.