Magister

Lucia Moser

Cybercrime-as-a-Service – A Business Model

VI.425

EDITIONS WEBLAW

ISBN 978-3-03916-257-4

Editions Weblaw
Bern 2024

Zitiervorschlag:
Lucia Moser,
Cybercrime-as-a-Service – A Business Model,
in: Magister, Editions Weblaw, Bern 2024

Universität Zürich[UZH]

Seminar Transnational Organised Cybercrime
Supervised by Prof. Dr. iur. Gian Ege
and MLaw Gishok Kiritharan

Cybercrime-as-a-Service – A Business Model

AN ANALYSIS OF A MODERN CYBER BUSINESS MODEL, THE THREATS IT POSES, AND THE POSSIBILITIES TO COMBAT IT

Master's Thesis
Submitted by

Lucia Andrea Moser
[redacted]
[redacted]
lucia.moser@uzh.ch
[redacted]

10th Semester
4 May 2024

Table of Contents

List of Abbreviations

ACM	Association for Computing Machinery
AGC	Amazon gift card
AI	Artificial Intelligence
ATM	Automated Teller Machine
BBC	British Broadcast Corporation
BBI	Bundesblatt der Schweizerischen Eidgenossenschaft
BFS	Bundesamt für Statistik
BKA	Bundeskriminalamt
bln	billion
CaaS	Cybercrime-as-a-Service
CSAM	child sexual abuse material
CVSS	Common Vulnerability Scoring System
DDoS	Distributed Denial of Service
DNS	Domain Name System
Ed.	Editor
EFD	Eidgenössisches Finanzdepartement
Eds.	Editors
EJPSS	European Journal of Political Science Studies
ENISA	European Union Agency for Cybersecurity
et al.	et alteri
etc.	et cetera
ETH	Eidgenössische Technische Hochschule Zürich
EU	European Union
EUR	Euro
EUROPOL	European Union Agency for Law Enforcement Cooperation
FBI	Federal Bureau of Investigation

HAL	Hyper Articles en Ligne
hr	hour
i.e.	in example
Id.	Idem
Ibid	Ibidem
IEEE	Institute of Electrical and Electronics Engineers
IJSIA	International Journal of Security and Its Applications
IP address	Internet protocol address
IT	Information Technology
JMLC	International Journal of Machine Learning and Cybernetics
MISQ	Management Information Systems Quarterly
Mr.	Mister
NATO	North Atlantic Treaty Organisation
NSA	National Security Agency
NZZ	Neue Zürcher Zeitung
p.	and the following page
pm	personal message
PP	PayPal
PSN US	U.S. PlayStation store
pw	password
RAT	Routine Activity Theory
SIAK-Journal	Sicherheitsakademie-Journal
SRF	Schweizer Radio und Fernsehen
SVR	Russian Foreign Intelligence Agency
TOR	The Onion Router
U.S.	United States of America
UN	United Nations

UN Cybercrime Convention	UN Convention on Countering the Use of Information and Communications Technologies for Criminal Purposes
UNODC	United Nations Office on Drugs and Crime
UNTOC	United Nations Convention against Transnational Organised Crime
USD	US-Dollars
VPN	virtual private network
WWW	World Wide Web

1. Introduction

In recent years, there has been a shift from offline to online crime, caused by the increasing digitalisation.[1] This shift can also be observed in the Swiss Crime Statistics, as cases have increased by 30% since 2021.[2] There is, however, an increase in cases on a global scale which can, in some part, be attributed to the Cybercrime-as-a-Service model.[3]

With the development of a new service model called "Cybercrime-as-a-Service" (CaaS), cybercrime has become accessible to almost everyone as all parts of a cyberattack can now be purchased in an underground marketplace.[4] With this increasing availability of CaaS, more and more companies, including critical infrastructure (power grids, financial services, energy providers, defence, health care, etc.), are exposed to the threat of a cyberattack.[5] The perpetrators also focus on confidential information from governmental institutions.[6] It has been said that CaaS will fuel most cyber threats in the future.[7]

The CaaS model has also led to the forming of cybercriminal groups.[8] In such a group, the attackers divide the work amongst themselves.[9] Therefore, an attacker becomes an expert in his field and his attacks get more sophisticated.[10]

CaaS has made the cybercrime phenomenon a highly organised system and is cross-cutting throughout all sub-areas of cybercrime.[11] This new phenomenon is significantly responsible for the increase in cybercrime cases and is still evolving.[12] It poses a threat to everyone and is, therefore, worthwhile taking a closer look at this topic.[13]

---

[1] MARKWALDER, 60; MEYWIRTH, 355.
[2] BFS (2021), 58; BFS (2022), 58; BFS (2023a), 62.
[3] MORGAN; SOOD/ENBODY, 29.
[4] HUANG/SIEGEL/MADNICK, 13, 29.
[5] BBI 2023 1659, 7; EUROPOL (2016), 39; HUANG/SIEGEL/MADNICK, 2.
[6] MEYWIRTH, 357.
[7] JIROVSKÝ et al., 2.
[8] Ibid.
[9] BKA (2020), 45; WAINWRIGHT/CILLUFFO, 2.
[10] HUANG/SIEGEL/MADNICK, 14 p.
[11] EUROPOL (2017), 17; MANKY, 9.
[12] SOOD/ENBODY, 29; WAINWRIGHT/CILLUFFO, 2.
[13] GÜNAL RÜTSCHE, Question 10 (Interview, see Annex); SOOD/ENBODY, 29.

1.1. Research Question and Goals of the Paper

This project aims to give an overview and an understanding of the business model behind CaaS, how organised crime profits from this new way of collaboration, and the threats it poses to governments, companies, and individuals. Finally, it highlights a few strategies to combat CaaS.

The following four research questions build the basis for this project:

1. How does the Cybercrime-as-a-Service business model operate?
2. What effects does Cybercrime-as-a-Service have on traditional organised crime groups and on organised cybercriminal groups?
3. What are the threats posed by the Cybercrime-as-a-Service business model?
4. What strategies could be implemented to counteract these threats effectively?

1.2. Methodology

After gaining an overview of the topic and its subareas, it was possible to understand the threats posed by CaaS and the consequences this business model has on Organised Crime. Lastly, it was possible to think about feasible countermeasures. The interview with Mr. Serdar Günal Rütsche was a big help in terms of highlighting the relevant issues faced within practice.

A limitation of the research has been that CaaS is often only analysed in relation to another topic, which means that the authors discussed the topic of CaaS rather basically and superficially. With SOOD/ENBODY, AN/KIM, and MANSKE, there were, however, three authors that went into depth. These are the ones that this paper is mainly based on. Various publications from the European Union Agency for Law Enforcement Cooperation (Europol) and the German Bundeskriminalamt (BKA) have also been helpful sources. As the research on the topic is limited, the available quantitative data is also limited. Different countries have analysed different aspects of the issue. Consequently, this paper will present a range of empirical evidence drawn from these different sources.

2. Foundation for Cybercrime-as-a-Service

2.1. Change in People's Behaviour

With the rise of mobile communication, there has been a shift in people's ways of communicating and behaviour, which has promoted an increase in cybercrime.[14] The more people and the economy interact with each other online, the higher the possibility of becoming a victim of a cyberattack.[15]

As more goods and services are bought via online shopping, the possibilities for cybercriminals have risen.[16] In Austria, the percentage of people buying things online was estimated at 70% for 2017.[17] All that data on credit cards, addresses, or other personal information is fed to the internet through these transactions.[18] The importance of such data will be discussed later (see section 3.2.3).

In 2023 96% of the Swiss population between the ages of 16-74 years used a smartphone or mobile phone to get access to the internet.[19] 68% used a laptop to do so.[20] A comparison was made in 2021 of Western European countries.[21] All of them had a usage around or above 80%.[22] This finding shows the number of potential devices that can be used for a cyberattack.

2.2. Evolution of Cybercrime

Over the last few decades, there have been four significant steps in the evolution of cybercrime.[23] The first step in the transnational organised cybercrime landscape was the exploitation of ATMs.[24] This was done on a local level for economic purposes.[25] In this phase, there was usually one single

---

[14] HUBER, 10, 18.
[15] HUBER, 13.
[16] HUBER, 10.
[17] HUBER, 11.
[18] HUBER, 11; MEYWIRTH, 357.
[19] BFS (2023b).
[20] Ibid.
[21] Ibid.
[22] Ibid.
[23] BRODOWSKI, 337.
[24] Ibid.
[25] Ibid.

perpetrator active.[26] In the next step, the internet was born and equipped criminals with new possibilities.[27] Then, cybercrime developed into an economy where cybercriminals could cooperate on a case-by-case basis.[28] This phenomenon is known as Cybercrime-as-a-Service.[29] The last step up until today is the increasing cooperation between transnational organised crime and cybercriminals.[30]

3. Cybercrime-as-a-Service

The term Crime-as-a-Service not only incorporates the offering of tools for cybercrime attacks (Cybercrime-as-a-Service) but also the selling of illicit goods such as illegal drugs, trading in weapons, forged documents, and child sexual abuse material via the internet.[31] This project will, however, only focus on the Cybercrime-as-a-Service aspect. If the word is of Crime-as-a-Service or CaaS only Cybercrime-as-a-Service is meant from here on.

In the cybercrime landscape, there has to be differentiated between cyber-dependant and cyber-enabled crimes.[32] Cyber-dependant crimes are those offences that can only be committed because of the internet.[33] They don't exist in the analogue world, for example, hacking or Distributed Denial of Service attacks (DDoS).[34] The counterpart are cyber-enabled crimes.[35] They can be committed in the analogue world.[36] With the rise of the internet, they have evolved from a local to a global phenomenon.[37] An example would be the distribution of child abuse material or the trading of forged documents.[38]

---

[26] BRODOWSKI, 338.
[27] Ibid.
[28] Ibid.
[29] SOOD/ENBODY, 30.
[30] BRODOWSKI, 337.
[31] WAINWRIGHT/CILLUFFO, 2.
[32] LEUKFELDT/NOTTÉ/MALSCH, 60.
[33] HUBER, 22; LEUKFELDT/NOTTÉ/MALSCH, 60.
[34] HUBER, 22; UNODC (What is it?).
[35] HUBER, 22; LEUKFELDT/NOTTÉ/MALSCH, 60.
[36] HUBER, 22; UNODC (What is it?).
[37] UNODC (What is it?).
[38] WAINWRIGHT/CILLUFFO, 2.

Cybercrime-as-a-Service can only be committed as a cyber-dependant crime as it offers precisely those tools to commit such a crime.[39]

To understand the threats CaaS poses, examining how the CaaS business model functions is essential. As cybercrime is a very dynamic market, it is only natural that CaaS is also a fast-changing and adapting topic.[40]

Crime-as-a-Service has been defined as "a business model used in the underground market where illegal services are provided to help underground buyers conduct cybercrimes in an automated manner"[41]. The sold service is designed and built by a technically skilled producer.[42] For clarification reasons, the definition needs to be amended to:

> CaaS is a business model used in the underground market where illegal services are provided by a technically skilled producer to help underground buyers conduct cybercrimes.

The following chapters will analyse the different aspects of this definition.

3.1. The Underground Market

One of the primary business models driving the cybercrime underground market is CaaS.[43] The selling of CaaS is made possible through underground markets.[44] Therefore, to understand how CaaS works and gets sold an understanding of the underground economy is beneficial.

Underground economies are the foundation for the trade in CaaS.[45] The lack of transparency and regulations and the internet's global reach enable illegal activities to thrive.[46] CaaS is primarily sold in marketplaces located either in the deep or the dark web.[47]

---

[39] LEUKFELDT/NOTTÉ/MALSCH, 60.
[40] EUROPOL (2015), 38; WAINWRIGHT/CILLUFFO, 2.
[41] SOOD/ENBODY, 28.
[42] JOHNSEN/FRANKE, 1.
[43] AN/KIM, 22637; WAINWRIGHT/CILLUFFO, 2.
[44] AN/KIM, 22637.
[45] SOOD/ENBODY, 22636.
[46] BOSTON CONSULTING GROUP; MANSKE, 235.
[47] MEYWIRTH, 355; WAINWRIGHT/CILLUFFO, 2.

3.1.1. The World Wide Web

The World Wide Web (WWW) is divided into three subwebs.[48] The clear web is the part of the WWW that is visible and available to everyone through search engines.[49] It has been estimated that this part makes up as little as 0.03% of the total WWW.[50] The remaining part is made up of the deep web.[51] The deep web is contrary to the clear web, which is inaccessible to all as it is usually protected through a password or a paywall.[52] Netflix and e-banking accounts would be two examples.[53] The dark web is not even accessible through regular browsers as it is even further below the surface.[54] A very well-known network to access the dark web is The Onion Router (TOR), which allows the user to hide his identity and location as well as any other information that would otherwise be freely available.[55] Hiding the information also means that it is harder for law enforcement agencies to identify a person behind a username.[56] Most of the illegal activities are happening in this part of the WWW.[57]

3.1.2. The Functioning of the Underground Economy

The underground economy is essentially ruled by supply and demand, just as any legitimate economy.[58] The quality of the services or products offered is attempted to be guaranteed through a rating system that is also used on legal trading platforms.[59] The better the rating, the more people will buy a specific service or product at a given price.[60] Similar to the legal market, a buyer will look for the service with the greatest potential to earn the desired profit at the lowest price.[61]

---

[48] KAUR/RANDHAWA, 2.
[49] Ibid.
[50] KAUR/RANDHAWA, 2; MEYWIRTH, 355.
[51] MEYWIRTH, 355.
[52] KAUR/RANDHAWA, 3; MEYWIRTH, 355.
[53] KAUR/RANDHAWA, 3.
[54] Ibid.
[55] GRECO/GRECO, 28; WAINWRIGHT/CILLUFFO, 2.
[56] WAINWRIGHT/CILLUFFO, 2.
[57] EUROPOL (2021b), 39; KAUR/RANDHAWA, 3; MEYWIRTH, 355.
[58] AN/KIM, 22638; MANSKE, 235.
[59] MANSKE, 236.
[60] Ibid.
[61] WAINWRIGHT/CILLUFFO, 4.

A good reputation is crucial for any seller and buyer in the underground market, as these transactions are illegal by their definition.[62] It is the only option to build trust and engage in a business transaction later on.[63] A buyer will only trust a seller he knows will make good on his offer, as he cannot report any wrongful behaviour to the police.[64]

As everyone engaging in the underground economy is aware of the illegality of the transactions, they take care to operate anonymously.[65] Anonymous doesn't mean the involved people don't know whom they are dealing with.[66] They might be unaware of a person's appearance or not know each other personally. However, they do know that user CC248, for example, is very capable of designing malware for Apple devices.[67] The involved people can mask their identities and hide their data through specific encryption tools.[68] Offline contacts and close geographic proximity are, however, very beneficial for the growth of a cybercriminal group.[69] LEUKFELDT et al. analysed 39 cybercriminal networks and found that 29 of them originated or expanded solely or mainly through offline social contacts.[70] Pre-existing social relationships often form the foundation for the origin and growth of common criminal activities, as there is already existing trust between the co-offenders.[71]

On the dark web, products and services are offered.[72] Products include illicit drugs, child pornography, weapons trafficking, and other nefarious items which illegally generate profit.[73] Additionally, two types of services are sold.[74] Firstly, there is Crimeware-as-a-Service.[75] In broad terms, it is designed to attack an infrastructure in cyberspace using a loophole in the system or a person's

---

62 EUROPOL (2014), 20; UNODC (Criminal Groups engaging in Cyber Organized Crime).
63 EUROPOL (2014), 20.
64 UNODC (Criminal Groups engaging in Cyber Organized Crime).
65 SUNDE, 71.
66 GÜNAL RÜTSCHE, Question 3.
67 Ibid.
68 WAINWRIGHT/CILLUFFO, 2.
69 UNODC (Criminal Groups engaging in Cyber Organized Crime).
70 LEUKFELDT/LAVORGNA/KLEEMANS, 292 p.
71 LEUKFELDT/LAVORGNA/KLEEMANS, 293.
72 AN/KIM, 22638; FAIRMAN, 14.
73 FAIRMAN, 14; NAZAH et al., 171796.
74 AN/KIM, 22638.
75 AN/KIM, 22638; HUBER, 87.

vulnerability.[76] One example of crimeware would be a kit to conduct phishing attacks (see 3.2.7.a).[77] Secondly, there are services, i.e., malware, designed to evade preventive measures taken by companies such as antivirus software.[78] These two services make up the Cybercrime-as-a-Service model.[79] An analysis has shown that 16% of all posts in underground forums contained offers for CaaS.[80] In the last few years, there has been an increasing shift from a product-oriented market, selling drugs and counterfeit goods, among other things, towards a market selling services.[81]

3.1.3. Advantages of the Underground Economy

One advantage of the underground marketplaces is that they work with cryptocurrencies like Bitcoin.[82] Almost all transactions are done through cryptocurrencies as they are convenient, international, anonymous, and irreversible.[83] It also simplifies the process of money laundering (see 3.2.9).[84]

Another advantage is that the costs of running an underground business are negligible.[85] Since the hosting websites of the marketplaces are located on compromised domains, the costs for the seller are non-existent, and in turn, the costs for CaaS stay low.[86]

3.2. The Service – The Nine Pillars of CaaS

CaaS includes the offering of "complex cyber security related services"[87]. It is, above all, defined by its multi-layered nature and complexity.[88] These services are either rented, sold, or leased to an interested third party.[89]

---

[76] AN/KIM, 22638; HUBER, 87.
[77] JOHNSEN, 3; UNODC (Cyber Organized Crime Activities).
[78] AN/KIM, 22638.
[79] Ibid.
[80] AKYAZI/VAN EETEN/GAÑÁN, 3.
[81] AN/KIM, 22636; WAINWRIGHT/CILLUFFO, 2.
[82] EUROPOL (2021c), 11; SOOD/ENBODY, 30.
[83] SOOD/ENBODY, 30.
[84] Ibid.
[85] Ibid.
[86] Ibid.
[87] JIROVSKÝ et al., 2.
[88] SINN et al., 41.
[89] FAIRMAN, 14; JOHNSEN/FRANKE, 1; MANKY, 10.

Performing a successful cyberattack has become increasingly difficult as companies and possible victims employ more complex and increasingly sophisticated security measures.[90] Therefore, the skills necessary to perform a successful attack have increased as well.[91] As fewer and fewer people are able to build the tools for an attack, the experts sell their attack tools on the black market to provide less skilled hackers with the means necessary to carry out a successful attack.[92] The result is that everyone, even people with no understanding of the technology behind it, can buy the essential tools and then commit a cyber-related crime.[93] This leads to a shallow entry barrier for amateurs.[94] The whole process of cyberattacks gets automated because everyone can buy it ready to use.[95]

The range of services offered is vast.[96] In every field, a specialist focuses on his specific skill set.[97] The BKA has identified nine pillars (Figure 1) to which all types of CaaS can be attributed:[98]

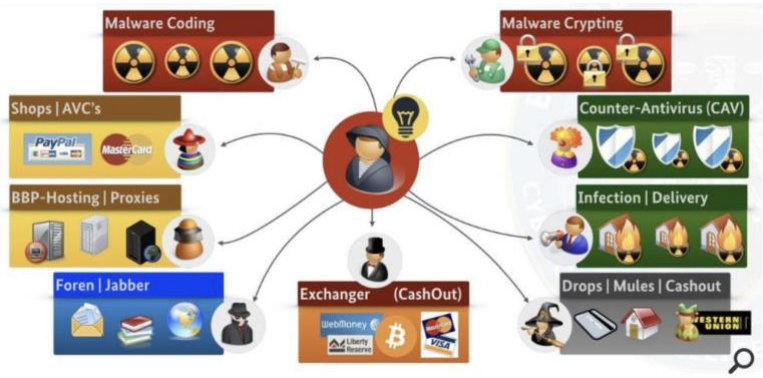

Figure 1: The nine pillars according to BKA[99]

[90] MANSKE, 235.
[91] MANSKE, 236.
[92] JOHNSEN/FRANKE, 1; MANSKE, 236.
[93] HUANG/SIEGEL/MADNICK, 2; LIGGETT et al., 103; MEYWIRTH, 355.
[94] EDMONDSON.
[95] MICROSOFT, 8; SOOD/ENBODY, 28.
[96] WAINWRIGHT/CILLUFFO, 2.
[97] MANSKE, 236; MEYWIRTH, 358.
[98] BKA (2020), 45 p.
[99] BKA (Cybercrime).

3.2.1. Forum and Jabber Server

The first pillar provides cybercriminals with the necessary contacts.[100] That happens through various forums and Jabber servers.[101] A Jabber server is a messaging service.[102] These forums or Jabber servers act as digital spaces to get in touch with a fellow cybercriminal and exchange contact information.[103] The BKA described them as the address book for cybercriminals.[104] Often, one needs a contact or be recommended by someone to gain access to a specific forum.[105] Once a criminal has gained access to a secret forum, he will have access to the services offered.[106] This initial point of contact is usually located in the clear web.[107] In these forums or Jabber servers, products are rated by consumers.[108]

Table 1 shows a compilation of various services being sought or offered as they have been posted in an underground forum.

Product/Service	Thread heading	Content of the post
Botnet-as-a-Service	Need Bots -Not Tons Dns Died	Looking to buy some bots anywhere from 100-1k since my old DNS died, I lost all my bots. I can pay via PP only. Please pm or post with how many you have and how much. Thank you
Bulletproof hosting-as-a-Service	Need offshore hosting!	Title says it all. I am looking to buy offshore hosting to host nulled scripts. Hit me up at axxx@live.com
Hacker-as-a-Service	Willing to pay for yahoo email hack	I need someone to help me by getting an e-mail pw for me. I'm willing to pay this is extremely urgent.
Obfuscation-as-a-Service	Crypting Service FUD.net $1.5	Hello, I offer fourth encryption service for $1.5 in .net touche skype: rxxxx
Traffic-as-a-Service	Selling DDoS Services! $4/hr – Cheap!	Title says all, my booter will keep target down for hours on end. PM me if you are interested.
Exploit	PDF or WORD Exploit wanted!!!	I am looking to buy PDF or Word Exploit. Only serious Sellers or point me to where I can buy. I know

[100] BKA (2020), 46.
[101] Ibid.
[102] JABBER.ORG.
[103] SOOD/ENBODY, 30.
[104] BKA (2020), 46.
[105] MEYWIRTH, 359; UNODC (Criminal Groups engaging in Cyber Organized Crime).
[106] AKYAZI/VAN EETEN/GAÑÁN, 8.
[107] MEYWIRTH, 356.
[108] EUROPOL (2017), 60; MANSKE, 236.

		they do not come cheap so do not tell me how expensive they are. Be ready to show proof and test, I do not have time for time wasters place. Hit me up folks. One thing, I hope this is not against the rules ae!
Cash-out/exchange	[H] $80 PP [N] $100 AGC or PSN US	As the title states, I have $80 PayPal and am looking to get either $100 amazon gift card US or $100 for the US PlayStation store

Table 1: Posts about sought and offered services[109]

3.2.2. Bulletproof Hosting, Proxy Providers, and VPN

To perform an attack, one needs an infrastructure from where the attack can be launched.[110] In this step, a hacker hides his IP address through a virtual private network (VPN) or proxy servers.[111] A proxy hides a user's IP address to enable (almost) anonymous browsing on the WWW.[112] A VPN ensures a secure connection to the internet through the usage of proxies and encryption tools.[113]

The attacker needs a whole server as infrastructure for more complex cyberattacks such as malware.[114] This infrastructure needs to be secure, anonymous, and resistant to law enforcement detection.[115] Providing this infrastructure is called Infrastructure-as-a-Service.[116]

Bulletproof servers not only host the tools for CaaS but also child sexual exploitation material and other illicit goods.[117] Legitimate service providers will shut down any such illegal activities on their servers.[118] One of the main offerings of bulletproof hosting is that the providers do not ask too many questions and will not stop any unlawful business.[119] These servers are often located in countries where the cyberlaws are either weak or non-existent, i.e.,

[109] AKYAZI/VAN EETEN/GAÑÁN, 8.
[110] MANSKE, 236; UNODC (Cyber Organized Crime Activities).
[111] EUROPOL (2016), 46; MANSKE, 236.
[112] AN/KIM, 22640.
[113] Ibid.
[114] MANSKE, 236.
[115] EUROPOL (2014), 19; EUROPOL (2017), 60; MEYWIRTH, 357.
[116] EUROPOL (2014), 21.
[117] EUROPOL (2014), 21; EUROPOL (2017), 60.
[118] HYSLIP, 832.
[119] Ibid.

Eastern Europe and Russia.[120] A bulletproof hoster is rented out for USD 5-700 per month, depending on the use and if the provider owns the server or uses an already compromised one.[121]

A few years ago, a group was operating such a bulletproof hoster from inside a former NATO bunker.[122] Its sole purpose was to host criminal websites and to hide them from law enforcement.[123] These websites offered illegal substances or forged documents and were used to organise and execute big cyberattacks.[124]

3.2.3. Marketplaces

To perform a cyberattack, criminals mostly rely on compromised access data, i.e., e-mail or social media accounts, credit card information, delivery addresses, or servers.[125] In order to perform a cyberattack, such data is crucial.[126] The offered data includes all kinds of available information on arbitrary people, such as credit card and bank details, as well as addresses, phone numbers, and other personal information.[127] Nowadays, this information is available on specialised websites, so-called marketplaces.[128] These are typically located in the deep web.[129] A few years ago, the criminal had to look through all the data himself, which took up much time.[130] With CaaS, this has become an automated process supplied by specialised people.[131]

The marketplaces can be found on the dark web in hacker forums and shops.[132] In these marketplaces, one can buy anything related to crime, from child pornography to weapons to CaaS.[133] The platforms are similar to legitimate

---

120 EUROPOL (2017), 60; HYSLIP, 833; SOOD/ENBODY, 32.
121 BKA (2021), 8.
122 BKA (2021), 10.
123 Ibid.
124 Ibid.
125 MANSKE, 236.
126 EUROPOL (2021), 12; EUROPOL (2023a), 9.
127 EUROPOL (2014), 21 p.
128 BKA (2020), 46; MANSKE, 236.
129 MEYWIRTH, 356.
130 MANSKE, 236.
131 Ibid.
132 HYSLIP, 833.
133 BKA (2020), 46; FAIRMAN, 14; NAZAH et al., 17.

online platforms, such as Amazon, with rating systems, customer service, and special discounts.[134]

In 2021, it has been estimated that around 184 million user accounts have been compromised and sold in the underground market.[135] All this compromised data has made it possible for buyers only to purchase precisely the data needed for their attack.[136]

3.2.4. Malware Development and Coding

Almost no cyberattack that is directed against the internet (cyber-enabled crime) is done without the use of malware.[137] For this reason, this paper's primary focus will be malware from here on.

Malware is a malicious software.[138] Put simply, its purpose is to cause damage to one or multiple networks or devices by sabotaging, stealing, or deleting data.[139] Some legitimate companies build malware in-house to test their cybersecurity measures.[140] In a criminal context, it is designed to harm and damage the victim's device or network.[141] It does so by using a system's vulnerability and then exploiting its data.[142] Malware has had to be adapted and needed to become more sophisticated as antivirus measures have increased their quality significantly.[143]

The malware landscape is expanding, with malicious software taking on an ever-greater variety of shapes and sizes.[144] The European Union Agency for Cybersecurity (ENISA) has reported the detection of 230,000 new malware strains every day in 2020.[145] Detecting malware is made more challenging as it

---

134 BKA (2020), 46; SUNDE, 71; UNODC (Cyber Organized Crime Activities); WAINWRIGHT/CILLUFFO, 3.
135 BKA (2021), 12; HASSO-PLATTNER-INSTITUT.
136 MANSKE, 236.
137 EUROPOL (2016), 17; MANSKE, 236.
138 RAZAK et al., 59.
139 EUROPOL (2021b), 38; RESHMI, 1.
140 HYSLIP, 827.
141 RESHMI, 1.
142 RAZAK et al., 59.
143 MANSKE, 235.
144 BKA (2022), 13.
145 ENISA (2020a), 9.

is designed to change after it has gained access to a system to avoid detection by the compromised device.[146] Known examples of malware are Trojan horses and viruses.[147]

A possible buyer plans his needed crimeware and then searches for a hacker who can design and build said crimeware.[148] The price of any CaaS is, in part, also determined by its complexity.[149] For malware, the price that must be paid depends on the time spent to program the malware.[150] In 2020, the price for a relatively basic malware was around EUR 5,000.[151]

3.2.5. Malware Crypting

In the next step, the buyer needs to ensure that his malware will not be detected by an antivirus software.[152] This is done through the so-called "obfuscation" process, where the malware's code is camouflaged.[153] This process of repackaging is called "crypting".[154] It is typically done by a different person than the one who created the malware.[155] He is called a "crypter".[156] In many cases, the crypter offers technical assistance later on to improve the crypting should it have been detected in too many instances.[157]

3.2.6. Counter-Antivirus-Services

It is in the highest interest of any perpetrator that his malware is not detected by antivirus software.[158] Specialised people offer to test the malware by running it through multiple antivirus programs to ensure its quality.[159] This outcome will, however, not be reported to the antivirus software developer as it would

---

146 ALRZINI/PENNINGTON, 1239; BKA (2022), 13.
147 RAZAK et al., 59.
148 BKA (2020), 46; MANSKE, 236.
149 MANKY, 9.
150 MANSKE, 237.
151 BKA (2020), 46.
152 AN/KIM, 26640; MANSKE, 237.
153 BKA (2020), 46.
154 AN/KIM, 26640; MANSKE, 237.
155 MANSKE, 237.
156 AN/KIM, 26640; MANSKE, 237.
157 MANSKE, 237.
158 MANSKE, 237; MEYWIRTH, 358.
159 BKA (2020), 46; MANSKE, 237; MEYWIRTH, 357.

defeat the whole purpose of the testing.[160] With these tests, the perpetrator stays up to date on the hazardousness of his malware and will know when he needs to develop his malware further.[161]

3.2.7. Malware Delivery and Infection on Demand

To use the malware, it needs to be run or installed on a victim's device.[162] The installation is often done through spam messages in the form of phishing or drive-by-infection.[163] A drive-by infection occurs when malware is downloaded when the victim visits a malicious website.[164] To successfully gain access, the malware exploits a vulnerability in a system where it alters, steals, or deletes data from a device.[165]

The way a cybercriminal or a criminal business earns money in this stage is very diverse: They either get paid when they sell a service, they sell monthly subscriptions to botnets, for example, or they might take a percentage of all successful attacks committed by the buyer.[166]

The following pages will look at a few selected attack and infection methods.

a. Phishing Attack

"Phishing is a scalable act of deception whereby impersonation is used to obtain information from a target"[167]. The perpetrator tricks the victim into thinking that a fraudulent message stems from a legitimate source and lures the victim into providing sensitive data.[168] In this context, it is also often talked of social engineering attacks.[169] This modus operandi is put together by the words "password" and "fishing", which describe the purpose of this method rather well.[170]

---

[160] MANSKE, 237.
[161] MANSKE, 237; MEYWIRTH, 358.
[162] MANSKE, 237.
[163] BKA (2020), 46.
[164] AN/KIM, 22640.
[165] RAZAK et al., 59.
[166] JIROVSKÝ et al., 2.
[167] LASTDRAGER, 8.
[168] CHAUDHRY/CHAUDHRY/RITTENHOUSE, 249.
[169] SALAHDINE/KAABOUCH, 2.
[170] AN/KIM, 22639.

The phishing can be distributed through text or social media messages, emails, or telephone calls.[171] The most common one being emails.[172] As it is so simple in its execution, it is the most favoured way to attack a system by cybercriminals.[173] For example, the perpetrator sends an email demanding that the victim update his payment methods on Netflix, or he sends a text message asking for money to deliver a package.[174] Such phishing messages can be seen in Figure 2.

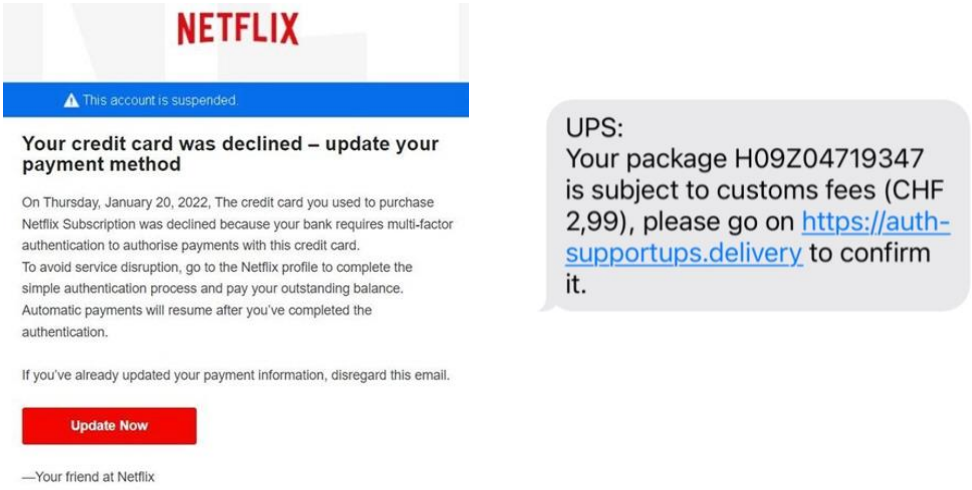

Figure 2: A Netflix scam email[175] (left) and a fraudulent text message from UPS[176] (right)

With approximately more than 3.4 billion spam e-mails containing phishing links sent daily, phishing is presently the most common form of cybercrime.[177] It is assumed that this amounts to 80% of all e-mail traffic.[178] Most of them are sent through so-called botnets.[179] A successful phishing attack leads to stolen credit card information and hijacked accounts of all kinds, ranging from social media accounts to passwords for online banking.[180]

Phishing emails often take advantage of current international situations, such as the Ukraine War, and use it as a theme in their messages.[181] However, by

---

[171] ALKHALIL et al., 7; BKA (2021), 14.
[172] MICROSOFT, 21.
[173] BKA (2021), 13.
[174] ALKHALIL et al., 5.
[175] Ibid.
[176] Private screenshot from the author, 05.02.2024.
[177] EUROPOL (2019), 51; FBI, 8, 20; GRIFFITHS.
[178] HOQUE/BHATTACHARYYA/KALITA, 2242 p.
[179] HOQUE/BHATTACHARYYA/KALITA, 2242 p.; SOOD/ENBODY, 36.
[180] KONRADT/SCHILLING/WERNERS, 1.
[181] BKA (2022), 11.

creating a similar or identical-looking website, they frequently imitate legitimate businesses, such as DHL, LinkedIn, Microsoft, Google, or Netflix.[182] The number of so-called phishing websites has increased over the last few years.[183] Figure 3 shows the development of the number of phishing websites since 2019.

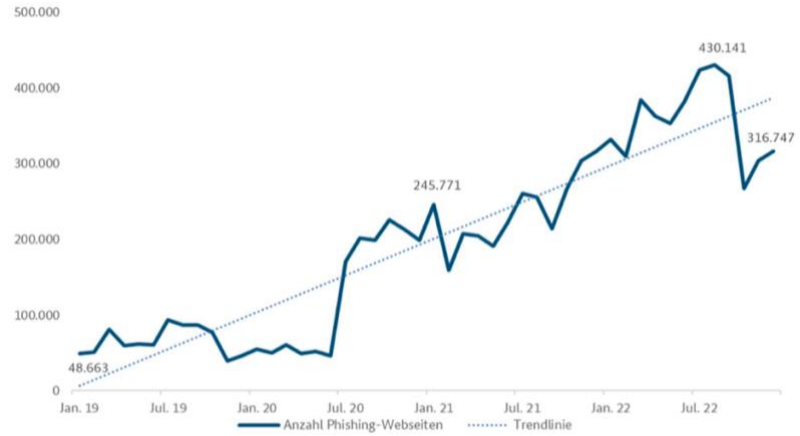

Figure 3: Number of phishing websites since 2019[184]

Phishing messages have become more sophisticated and, therefore, more challenging for a person to spot.[185] On the other hand, it has become much more difficult to successfully deliver such a message due to the increased security measures.[186] If a perpetrator wants to install malware through a phishing attack, he, therefore, only pays for every successful installation of malware.[187] The price for infection costs approximately USD 100 for 1,000 successful installs.[188] If the perpetrator wants to infiltrate the targeted device or network himself, he can buy a phishing kit containing all the tools needed.[189]

Even though the concept behind phishing is a relatively simple one, it still poses a serious threat to companies, governments, critical infrastructure, and

[182] BKA (2022), 11; CHAUDHRY/CHAUDHRY/RITTENHOUSE, 248.
[183] BKA (2022), 11; MICROSOFT, 9.
[184] BKA (2022), 11.
[185] EUROPOL (2016), 33; EUROPOL (2021b), 43.
[186] EUROPOL (2014), 22; MANSKE, 237.
[187] Ibid.
[188] MANKY, 10; MICROSOFT, 9.
[189] JOHNSEN, 3; MICROSOFT, 8.

individuals, as phishing is often paired with malware infiltration.[190] In Germany, phishing was the most common entry vector for ransomware in 2022.[191]

b. Access-as-a-Service

A second way to gain access to a system or device other than through phishing is to make use of mistakes made in a specific software.[192] Taking advantage of such a weakness is called "exploit".[193] These exploits are then sold as Access-as-a-Service on the underground market.[194] If the developer has not identified a gap, this exploit is called a zero-day exploit, as the developer had zero time to patch up the gap.[195] The opposite is a n-day exploit where the developer is aware of the vulnerability but has not yet been able to "heal" the gap.[196] Zero-day exploits are sold for around USD 10,000 as they are more valuable than n-day exploits, which usually are offered for approximately USD 2,000.[197]

c. Ransomware

The most harmful form of malware is ransomware.[198] A ransomware attack encrypts the files on a device or a network or locks the device altogether and holds it hostage, demanding a ransom payment from the victim.[199] Cybercriminals often target critical infrastructure such as hospitals and schools.[200] According to the Federal Bureau of Investigation (FBI), 42% of all reported ransomware attacks targeted critical infrastructure in the U.S. in 2023.[201] The victims are often threatened with releasing the data onto the black market and simultaneously demand a ransom to decode the data.[202] This modus

---

190 BKA (2022), 11; MICROSOFT, 22.
191 BKA (2022), 11.
192 BKA (2021), 15.
193 Ibid.
194 Ibid.
195 WICKER, 99.
196 ELBAZ/RILLING/MORIN, 1.
197 BKA (2021), 15 p.
198 BKA (2022), 14.
199 PAQUET-CLOUSTON/HASLHOFER/DUPONT, 1; RESHMI, 1.
200 CHAINALYSIS, 11.
201 FBI, 13.
202 BKA (2021), 20; MANKY, 12.

operandi is called double extortion.[203] In order to get the key to decrypt the encrypted data, the victim has to pay the ransom.[204] Sometimes, the data gets sold on the black market nonetheless.[205]

The payment is usually made in a cryptocurrency.[206] These cryptocurrencies will also be later used to launder the money (see 3.2.9).[207] The total amount of ransomware payments made in 2022 amounted up to 457 billion USD.[208] Here is where the importance of cryptocurrencies comes in: If the victim of a ransomware attack would pay the perpetrator through a standard bank account, the money would be easily traceable leading to an arrest of the perpetrator.[209]

A prominent attack in the history of ransomware was the WannaCry ransomware attack in 2017.[210] A vulnerability in a Microsoft Windows system was used to launch an attack and demand a ransom.[211] It has affected more than 300,000 computers in 150 states and led to billions of dollars in damages.[212]

d. Distributed Denial of Service Attack

When a perpetrator has gained access to a device or system through a phishing attack or an exploit, it is possible that he does not use it to extort money from the victim.[213] Another option would be to rent the access out as part of a botnet.[214] A botnet is a net of many malware-infected devices that are controlled by one person called the botmaster.[215]

A DDoS attack is usually launched from a botnet.[216] Through the botnet, the botmaster can send an infinite number of requests to the victim network (often

---

[203] BKA (2021), 20.
[204] HYSLIP, 828.
[205] BKA (2021), 18.
[206] EUROPOL (2021c), 12; PAQUET-CLOUSTON/HASLHOFER/DUPONT, 1.
[207] EUROPOL (2021c), 3; MANSKE, 238.
[208] BKA (2022), 14.
[209] EUROPOL (2016), 11; JIROVSKÝ et al., 2.
[210] VOLZ.
[211] BBC.
[212] BBC; VOLZ.
[213] JIROVSKÝ et al., 2; LIGGETT et al., 103.
[214] Ibid.
[215] HOQUE/BHATTACHARYYA/KALITA, 2243; HUBER, 77.
[216] HOQUE/BHATTACHARYYA/KALITA, 2243.

websites), rendering it useless for a period of time.[217] Such an attack aims to disrupt the targeted network or website to hinder it from offering or performing its services.[218] This leads to poor user experience and can result in severe economic losses for the victim.[219]

Since the beginning of the war in Ukraine, DDoS attacks have increased again, especially against EU states that condemned Russia's aggression.[220] One example is the attack on the European Parliament in 2022 committed by a pro-Russian hacker group.[221] The website of the European Parliament had been unavailable for several hours.[222]

3.2.8. Drops, Mules, and Cash-Out

In this stage, the results of the cyberattack are transformed into real life money.[223] This is usually done through so-called money mules.[224] They are often part of the criminal organisation or are tricked into collaboration.[225] To find a money mule, a criminal organisation posts a fake job advert on a social media platform or a job forum, for example.[226] The people mainly targeted are students or other people belonging to population groups with no or little income.[227] Packages that contain forged documents, wrongfully ordered laptops, or similar need to be picked up at a drop site, or they may have to open a bank account.[228] The mules receive a percentage of the proceeds as payment.[229] This pillar has the most risks for the supplier as it is the only one that requires an action in the physical world.[230]

---

[217] HOQUE/BHATTACHARYYA/KALITA, 2242.
[218] Ibid.
[219] BHARDWAJ et al., 2.
[220] BKA (2022), 19; EUROPOL (2023b), 6.
[221] EUROPOL (2023b), 17; MEIJER/SIEBOLD.
[222] MEIJER/SIEBOLD.
[223] MANSKE, 238.
[224] EUROPOL (2016), 43.
[225] EUROPOL (2017), 61.
[226] ESOIMEME, 203; EUROPOL (Money Muling).
[227] EUROPOL (2017), 61; EUROPOL (Money Muling).
[228] ESOIMEME, 204; EUROPOL (2017), 61; HUANG/SIEGEL/MADNICK, 23; MANSKE, 238.
[229] MEYWIRTH, 358.
[230] EUROPOL (2017), 61; MANSKE, 238; MEYWIRTH, 358.

3.2.9. Exchanger

All money trails are erased to hinder law enforcement's ability to trace them as a final step.[231] This is often done through the acquisition and selling of cryptocurrencies.[232] The phenomenon is known and goes by the term Money-laundering-as-a-Service.[233] Money launderers need to have a deep understanding of the possible technologies and the provisions against money laundering.[234]

In a first step, the criminal proceeds are transferred into the financial system.[235] This is done, for example, through the bank account of a money mule by depositing the money into said bank account.[236] Secondly, the origins of the proceeds are layered to hide all traces of where it came from.[237] Cryptocurrency mixers break the links between the first and the last transaction and, with that, obfuscate the original IP address.[238] With global platforms, the exchange of one cryptocurrency into another is cheap.[239] The money gets transferred through several bank accounts opened by mules to erase the traces of origin.[240] Finally, when the laundered money is transferred back to the perpetrator, no traces of the relation to any crimes are left.[241] The laundered money is used in the licit economy, and it appears that the perpetrator received it through legal circumstances.[242]

---

231 JIROVSKÝ et al., 2; MANSKE, 238.
232 MANSKE, 238.
233 EUROPOL (2014), 22; UNODC (Cyber Organized Crime Activities).
234 MANSKE, 238.
235 UNODC (Cyber Organized Crime Activities).
236 ESOIMEME, 204.
237 UNODC (Cyber Organized Crime Activities).
238 EUROPOL (2021c), 10.
239 MANSKE, 238.
240 ESOIMEME, 204; EUROPOL (2017), 61; HUANG/SIEGEL/MADNICK, 23.
241 MANSKE, 238.
242 HUANG/SIEGEL/MADNICK, 23; MANSKE, 238; UNODC (Cyber Organized Crime Activities).

3.3. The Business Model behind Cybercrime-as-a-Service

3.3.1. In General

The CaaS model comprises a triangular relationship between the buyer, the producer, and, in some cases, an advertiser.[243] The producer is technically versed.[244] He designs crimeware and acts as the seller.[245] In some instances, he commissions an advertiser to promote his crimeware in underground marketplaces.[246] The buyer responds to the advertisement and buys the service.[247] It is an exchange of a service for money – or, in this case, cryptocurrencies – between cybercriminals.[248] Sometimes, the seller even provides training in the form of tutorials or consulting services.[249]

Usually, behind each of the three parties is an enterprise compiled by a few or a single person.[250] Cooperation with other hackers is in the interest of an individual hacker as it is possible, on the one hand, to reduce the risk of detection and, on the other, to maximize profits from attacks.[251] CaaS distinguishes itself, therefore, by a high division of labour between the people involved.[252]

These types of organisations have become increasingly more organised as the rewards gained from cybercrimes and CaaS have increased.[253]

3.3.2. An Individual as an Entrepreneur

CaaS leads to an increased specialisation of one hacker.[254] If this specialised hacker does need something additional, he buys it from someone else.[255] He

---

[243] SOOD/ENBODY, 30.
[244] Ibid.
[245] Ibid.
[246] Ibid.
[247] Ibid.
[248] MOYA/LANUZA, 26.
[249] LIGGETT et al., 103; MANKY, 9; MEYWIRTH, 356; WAINWRIGHT/CILLUFFO, 4.
[250] MANSKE, 235; SINN et al., 65.
[251] HUANG/SIEGEL/MADNICK, 2 p.
[252] BKA (2020), 45; WAINWRIGHT/CILLUFFO, 2.
[253] SOOD/ENBODY, 28; WAINWRIGHT/CILLUFFO, 2.
[254] BKA (2020), 45; MANSKE, 235; WAINWRIGHT/CILLUFFO, 2.
[255] EUROPOL (2017), 58; MICROSOFT, 8.

will build the parts he knows how to himself and outsource the other ones.[256] Once he has designed an attacking tool, he can sell it to a different buyer or use it to attack himself.[257] A seller no longer only profits from performing his own attack.[258]

Under normal circumstances, various hackers get together on a mandate basis for one project.[259] They aren't structured like a company but instead have a flat organigram.[260]

The individual can change from one organisation or collaboration to another more effortlessly than in a traditional organised crime group.[261] They can also be part of several groups at the same time.[262] The networks are not set in stone.[263] It has been voiced that it would be impossible for a single person to perform an attack alone as the victims have increased their security measures, and an attack has gotten too complex for one person alone.[264]

3.3.3. A Hierarchically Structured Company

The arrangement of a hierarchically structured company offering CaaS is similar to the structure of a legitimate company.[265] At the top, there is a Chief Executive Officer.[266] He often has an economics background and is good at maximizing profits but not necessarily versed in technological aspects.[267] He is supported by a Chief of Operations and a Chief of Finance.[268] They also have people working for them in product development and financial services.[269] A group might also be responsible for advertising services, the so-called

---

[256] BKA (2020), 45.
[257] HUANG/SIEGEL/MADNICK, 13.
[258] MANKY, 10.
[259] EUROPOL (2015), 12.
[260] AN/KIM, 22636; LAVORGNA, 118.
[261] LAVORGNA, 124.
[262] Ibid.
[263] AN/KIM, 22636.
[264] GÜNAL RÜTSCHE, Question 1; MANSKE, 235.
[265] SOOD/ENBODY, 29.
[266] WAINWRIGHT/CILLUFFO, 3.
[267] Ibid.
[268] Ibid.
[269] Ibid.

"crimevertisment".[270] Often, these companies outsource certain steps of the value chain and, therefore, make use of CaaS themselves.[271] They will do so to increase productivity.[272] Additionally, they also use traditional business methods such as discounts, customer service, and advertisement to increase their profits and improve a customer's experience.[273] Most of these groups consist of 5 to 10 perpetrators working together; however, there are also a few groups with more than 20 perpetrators.[274]

With this before-mentioned specialisation, the business group profits as a whole and is strengthened as a player in the market.[275] With the division of labour, the criminal groups will diversify their services, whereas the individual gets more specialised in the one service he offers.[276]

3.4. The Perpetrators

There are two groups in the underground CaaS market: the majority and the minority group.[277] Depending on the technological skills and knowledge one belongs to one group or the other. [278] If someone has the skills to create a crimeware themselves and therefore perform an attack alone or with minimal assistance, this person belongs to the minority group.[279] They are the ones selling the tools of an attack to unskilled perpetrators.[280] In turn, they only buy what they can't design themselves.[281]

With the increased quality of the security measures, the number of people who are able to build successful crimeware (i.e., malware) has decreased.[282] The majority group has little or no technical skills and depends on buying tools to

---

[270] SOOD/ENBODY, 31.
[271] MICROSOFT, 8; SINN et al., 67.
[272] MOYA/LANUZA, 26.
[273] MEYWIRTH, 356; WAINWRIGHT/CILLUFFO, 3.
[274] GÜNAL RÜTSCHE, Question 7; LEUKFELDT/LAVORGNA/KLEEMANS, 292.
[275] SINN/IDEN, 64 p.
[276] EUROPOL (2015), 8.
[277] JOHNSEN, 104.
[278] Ibid.
[279] BKA (2020), 45; JOHNSEN, 104; MANSKE, 235.
[280] JOHNSEN, 104.
[281] HUANG/SIEGEL/MADNICK, 13.
[282] MANSKE, 236.

perform a cyberattack.[283] They can then perform complex cyberattacks without a technical understanding of the process behind them.[284]

It is not only individuals who are perpetrating cybercrimes and using CaaS.[285] Some groups also work with states or function as state actors.[286] They also fall in this category if the state tolerates them.[287] One cybergroup called APT29 is assumed to be mandated by the Russian foreign intelligence service SVR.[288]

Some states are actively engaging in cybercriminal behaviour.[289] A prime example would be North Korea, which is financing its nuclear and missile programs by attacking cryptocurrency platforms.[290] It has also been assumed that the WannaCry ransomware attack (see 3.2.7.c) was launched from North Korea.[291]

3.5. The Victims

Possible victims are governments and its various institutions, companies, and individuals.[292]

Cyberattacks increasingly target governments.[293] The reasons here for are diverse. The governments store valuable data that is attractive to cybercriminals.[294] They are also seen as lucrative targets.[295] Some perpetrators are interested in sowing discord among the public as the government is responsible for the well-functioning of daily life.[296] Then there are also geopolitical reasons to name the example of the Ukraine war, where the aim is to disrupt governmental operations and national security.[297]

---

283 EUROPOL (2021b), 38; HUANG/SIEGEL/MADNICK, 13.
284 AN/KIM, 22637; HUANG/SIEGEL/MADNICK, 2; MANSKE, 235; SOOD/ENBODY, 28.
285 BKA (2021), 31.
286 BKA (2021), 31; UNODC (What is it?).
287 BKA (2021), 31.
288 BKA (2021), 32; NATIONAL CYBER SECURITY CENTER.
289 BKA (2021), 31.
290 EDER (2024); NICHOLS.
291 BBC.
292 HUBER, 18.
293 BUNDESRAT, 3.
294 EFD.
295 REED.
296 BKA (2021), 2; BUNDESRAT, 15; UNODC (What is it?).
297 EDMONDSON; REED.

Companies are not only targeted to be exploited but also to be part of a more extensive network like a botnet and can thus be used as a "vehicle for other criminal activities".[298] The financial sector is the most targeted one.[299]

In general, anyone using an internet connection can become a cyberattack victim.[300]

3.6. Reasons for the Rise of CaaS

To conclude this chapter, it can be said that with the rise of the internet and the anonymity it provides, cybercrimes can now be committed from everywhere in the world, anywhere in the world.[301] Therefore, CaaS has become more attractive as purchasing a needed service from someone on the other side of the planet is also possible.[302]

CaaS has enabled cybercriminals to earn more money than ever before through cybercrime.[303] With the anonymity and the possible financial reward from cybercrime, a growing number of people is attracted.[304] The profit from a successful attack mostly stays with the attacker as the costs are relatively low.[305] Criminals can now make money by performing attacks themselves and by selling the tools for an attack and their expertise to an undefinable number of other perpetrators.[306] It is possible to launch global attacks compared to previous attacks that were only regional.[307]

A few years ago, a cybercriminal had to possess many different skills to perform a successful cyberattack.[308] Now, he can focus on one task and improve this skill.[309]

---

[298] EUROPOL (2015), 8.
[299] BKA (2021), 13; EUROPOL (2019), 51.
[300] HUBER, 86.
[301] HONG KONG COMPUTER EMERGENCY RESPONSE TEAM COORDINATION CENTRE.
[302] Ibid.
[303] SOOD/ENBODY, 28.
[304] BRODOWSKI, 339; EUROPOL (2021b), 41.
[305] SOOD/ENBODY, 30.
[306] REID, 236.
[307] JIROVSKÝ et al., 2.
[308] WAINWRIGHT/CILLUFFO, 2.
[309] BKA (2020), 45; EUROPOL (2015), 8.

The evolvement of CaaS can also be traced back to the emergence of the dark web, the increasing demand for cybercriminal services, the sophistication of cybersecurity and cryptocurrencies.[310]

The increasing demand for cybercrime tools has allowed cybercriminal groups to thrive.[311] CaaS has also facilitated two or more groups to work together across borders.[312] However, it is also easier for a single person to operate on a freelance basis.[313]

4. Effects on Organised Crime

There is no definition of organised crime in the UNTOC.[314] This was done as such a definition would quickly be outdated.[315] The distinction is therefore made based on the definition of organised criminal groups.[316] Organised criminal groups have been defined in Article 2(a) of the UNTOC as "a structured group of three or more persons, existing for a period of time and acting in concert with the aim of committing one or more serious crimes or offences established in accordance with this Convention, in order to obtain, directly or indirectly, a financial or other material benefit".

The emergence of CaaS as a business model has led to a new form of organised crime that differs from traditional organised crime. Therefore, a distinction must be made between the organised cybercriminal groups in the context of CaaS and the traditional organised crime groups.[317]

4.1. The Role of Traditional Organised Crime Groups

Although the traditional organised group operates in the offline world, they also use the online world to communicate with each other and to facilitate their crimes.[318] Traditional crime groups are more stable compared to newly formed

---

310 ASSMAN; EUROPOL (2015), 9, 30; SOOD/ENBODY, 30.
311 JIROVSKÝ et al., 2.
312 EDMONDSON.
313 EUROPOL (2015), 9, 30.
314 UNODC (Actors involved).
315 Ibid.
316 Ibid.
317 LAVORGNA, 122.
318 LAVORGNA, 122; UNODC (What is it?).

cybercrime groups.[319] According to LAVORGNA, the empirical evidence is not so strong in suggesting that all the traditional organised crime groups have indeed moved their activities online.[320] The Italian Mafia, for example, has not significantly exploited cyberspace.[321] It is assumed that this is due to the fact that they operate through the means of violence, intimidation, and a code of silence.[322] They not only aim to profit, but they also want to mark their presence in their territory.[323] Cybercriminal groups are more challenging to discover as they are more resilient and more flexible.[324]

However, this does not mean that traditional crime groups don't use the possibilities connected with cybercrime.[325] They use the possibility of illicit online gambling, for example.[326] It has also become relatively easy and cheap to purchase any desired service and the tools connected with it online.[327] With all kinds of products readily available through cyberspace, this is also an opportunity for traditional crime groups to expand their business in the cyberworld.[328] The monetary gains connected to cybercrime have also attracted the interest of traditional groups.[329]

Although some traditional organised crime groups are actively involved in the cybercrime underground market, they are not the ones governing it.[330] A conventional organised crime group might work with a few non-members on a particular project.[331] Instead, they act as investors, helping with money laundering or assisting in specific cybercrime operations.[332]

---

[319] BRODOWSKI, 338; LAVORGNA, 124.
[320] LAVORGNA, 125.
[321] LAVORGNA, 126.
[322] Ibid.
[323] Ibid.
[324] SINN/IDEN, 64.
[325] UNODC (2013), 40; WAINWRIGHT/CILLUFFO, 4.
[326] GRECO/GRECO, 28; UNODC (Criminal Groups engaging in Cyber Organized Crime).
[327] WAINWRIGHT/CILLUFFO, 4.
[328] WAINWRIGHT/CILLUFFO, 2.
[329] BRODOWSKI, 339; EUROPOL (2021b), 41.
[330] LUSTHAUS, 180.
[331] BRODOWSKI, 339.
[332] LUSTHAUS, 180.

4.2. Organised Cybercrime Groups

This new form of organised criminal groups was not explicitly thought of when the UNTOC was created, as there is no mention.[333] Therefore, it needs to be examined if they fall under the definition of Article 2(a) UNTOC.

A structured group is defined in Article 2(c) as "a group that is not randomly formed for the immediate commission of an offence, and that does not need to have formally defined roles for its members, continuity of its membership or a developed structure". This term should not be used in a narrow sense but should also encompass groups without a hierarchy.[334]

The CaaS business model is organised as an economy.[335] There is a lot of change in the composition of the members, whereas a traditional organised crime group has high internal stability and a strong bond between the members.[336] There is no set hierarchy as they work on a project basis.[337] This has, however, also changed in some cases over the last few years, as some cybercriminals have built a company around their activities.[338] The definition mentioned above does not stipulate a hierarchy or a continuation of membership in cybercriminal groups.[339] The cybercriminal groups, therefore, also fulfil the UNTOC definition.[340]

4.3. Effects on the Structure of Organised Crime

To ensure the business works smoothly, it is still essential that each member knows their role.[341] Nowadays, cybercrime groups have organised themselves to provide the well-functioning of operations.[342]

CaaS has resulted in a shift towards more flexible, complex, and adaptable organised crime with regard to non-traditional organised crime groups.[343] With

---

[333] See UNTOC.
[334] MINAKAWA, 228; UN GENERAL ASSEMBLY, 2.
[335] MANKY, 9.
[336] BRODOWSKI, 339.
[337] AN/KIM, 22636; EUROPOL (2015), 12; LAVORGNA, 118.
[338] BRODOWSKI, 339.
[339] BRODOWSKI, 339; UNODC (Actors involved).
[340] Ibid.
[341] MANKY, 9.
[342] MANKY, 11.
[343] EUROPOL (2021b), 20; SINN et al., 171 p.

the anonymity in the dark web, the convenience of cryptocurrencies, and the amenities of cyberspace in general, it has become possible for a single person to launch their own attacks by buying the needed tools in an underground market.[344]

With the shift from offline to online crime, EUROPOL expects a collapse of the hierarchically structured groups.[345] The hackers will predominantly work on a mandate basis, meaning they will get together for one or more projects and then dissolve again.[346]

This tendency is also supported by the finding that since 2014 there has been a shift from structured to diffusely organised groups.[347] At that time, an attack was usually performed by a more or less closed group, meaning it was consistent in its members, and the perpetrators knew each other personally.[348] In 2021, about 60% of all groups active in the underground market were loosely structured groups or possessing a core group at most.[349] The remaining 40% were hierarchically structured groups.[350]

In 2020, it was unclear if the traditional organised crime groups had moved their business to cyberspace or if new groups had formed there.[351] In practice, it is seen that the conventional groups have now expanded into cyberspace as well.[352] However, there seems to be a consensus that the groups active in cyberspace will evolve to be rather loosely organised, not hierarchically structured, and the network will be fluid, leading to single entrepreneurs who work freelance.[353]

The evolution of technology and digitalisation has opened up the possibilities of exploitation for criminal groups, whether traditional or newly formed.[354]

---

344 SINN/IDEN, 64.
345 EUROPOL (2015), 8; MARKWALDER, 60.
346 EUROPOL (2015), 12.
347 MANSKE, 235.
348 Ibid.
349 EUROPOL (2021b), 20.
350 Ibid.
351 LAVORGNA, 177.
352 GÜNAL RÜTSCHE Question 21.
353 AN/KIM, 22637; EUROPOL (2015), 12; LAVORGNA, 118.
354 AN/KIM, 22637; EUROPOL (2015), 12.

5. Threats posed by Cybercrime-as-a-Service

Cybercrime, and with it, CaaS poses a variety of threats to governments, companies, and individuals.[355] The full scope of the threats that CaaS and its related topics pose cannot be depicted in this project as they would require a more profound knowledge of the processes in the underground markets on the one hand and more detailed research in other related fields on the other.

CaaS is only now developing and has not yet reached its full potential.[356] The increasing and facilitated availability could lead to it being more accessible to people not native to the dark web who would not engage criminally in the analogue world.[357] These threats are often related and similar to cybercrime as a whole.[358]

Some threats affect all the groups mentioned above. The rise of artificial intelligence (AI) also significantly impacts the evolvement of CaaS.[359] AI has been used to phrase phishing messages and the development of malware, making it harder for individuals to spot it as a fraudulent message.[360] According to the BKA, the attack tools are expected to develop further, and new attack modi operandi will come up, leading to an expansion of the business model.[361]

All successful attacks lead to an uncontrolled outflow of data on a big scale.[362] This data makes people, companies, and infrastructure a target for cyberattacks.[363]

5.1. Threats to Governments and Critical Infrastructure

The threats concerning governments affect the most people as governments are responsible for the well-functioning of everyday life.[364] Not only does it affect law enforcement, but it also affects national security.[365]

---

355 HUBER, 18.
356 GÜNAL RÜTSCHE, Question 10.
357 GÜNAL RÜTSCHE, Questions 10 and 11.
358 EDMONDSON.
359 BKA (2022), 30.
360 BKA (2022), 30; ENISA (2020b), 2.
361 BKA (2022), 30.
362 GÜNAL RÜTSCHE, Question 14.
363 EUROPOL (2023a), 9; HUBER, 11; MEYWIRTH, 357.
364 BUNDESRAT, 9, 15; EDMONDSON.
365 EDMONDSON.

Critical infrastructure is crucial for the well-functioning of any state, and the state is responsible for its protection.[366] Therefore, this section will deal with the threats connected to critical infrastructure, regardless of whether private companies operate some of those infrastructures.[367]

5.1.1. Threats to Governments

In November 2023, a Swiss company called Concevis became a victim of a ransomware attack.[368] They stored data of the Swiss Federal administration.[369] The attackers threatened Concevis with releasing the data into the dark web should they fail to pay the ransom.[370] It is self-explanatory that it is in no government's interest to have its data available on the dark web.

Some groups specifically target a state's infrastructure to spread distrust and interfere in internal affairs in other countries.[371] They are often mandated by another state.[372] One example is the involvement of the Russian government in the 2016 U.S. presidential elections, where they tried to infiltrate the electoral infrastructure.[373] They have attempted to "undermine public faith in the U.S. democratic process"[374].

As CaaS is sold from one person to another and layering networks are used throughout the various stages, the attribution process gets disrupted.[375] The one creating the tools to perform an illegal activity is not the one committing it.[376] This makes it harder for law enforcement to prosecute the person behind the malware creation.[377] As CaaS is a global phenomenon, jurisdictional issues are present in investigations, apprehension, and prosecution.[378]

---

366 BKA (2021), 2; BUNDESRAT, 15.
367 BBI 2023 1659,19; BUNDESRAT, 15.
368 EFD.
369 Ibid.
370 Ibid.
371 UNODC (What is it?).
372 Ibid.
373 DRÖSSER; NZZ.
374 KESSLER.
375 EUROPOL (2016), 57; SOOD/ENBODY, 36.
376 SOOD/ENBODY, 28.
377 SOOD/ENBODY, 36.
378 Ibid.

CaaS – and cybercrime in general – forces law enforcement to allocate some of the limited resources towards preventing and resolving CaaS-related crimes, leaving fewer resources for other fields.[379]

With the creation of an anonymous platform to exchange criminal services, the threshold for cooperation between terrorism and organised crime has been lowered.[380] It has become easier for them to use cybercrime services as well.[381]

5.1.2. Threats to Critical Infrastructure

As has been mentioned a few times, with the availability of the tools to perform a cyberattack, critical infrastructure is also exposed to a higher risk of attack.[382] This not only causes financial damage but also disrupts the well-functioning of the public bodies.[383]

In 2023, a ransomware attack was committed on Prospect Medical Holding, a U.S. healthcare provider.[384] Several hospitals had to suspend some of their services for the time being, while others had to close completely.[385] The ransomware group published the stolen data on the dark web shortly after.[386] This data included social security numbers, financial and legal documents, and medical files.[387]

5.2. Threats to Companies

A successful cyberattack adversely affects a business's reputation and the trust put in it by customers and business partners.[388] If a company's stored data ends up on the black market, customers and business partners will lose confidence in the company.[389] This leads to lower revenues.[390] Not only do the lost

---

379 EDMONDSON.
380 EUROPOL (2015), 12.
381 EUROPOL (2016), 49.
382 HUBER, 18; MEYWIRTH, 357; SINN et al., 66.
383 BKA (2021), 2.
384 KAPKO; SCHAPPERT.
385 SCHAPPERT.
386 KAPKO; SCHAPPERT.
387 KAPKO.
388 ASSMAN.
389 ASSMAN; HUBER, 77.
390 ASSMAN.

customers result in lower revenues, but the cyberattack also causes financial damage.[391]

Companies should, therefore, be well advised to invest in cybersecurity.[392] However, if a company does not see the immediate benefit, it will hesitate to invest a significant amount of money.[393] This mindset is, however, dangerous as it is not a question of if but when a company will be attacked.[394]

5.3. Threats to Individuals

An individual can also become a victim of a cyberattack that might have been facilitated through CaaS, such as a phishing attack.[395] Criminal groups target individuals by spamming to gain access to the desired personal data.[396] Cyberattacks are usually not targeted directly but result from luck.[397] Therefore, everyone can become a possible victim.[398] One becomes a victim when a mistake was made somewhere along the way.[399] A successful cyberattack leads, among others, to financial damage and loss of valuable data.[400]

6. Combating Strategies

It has been said that there are only two types of businesses: the ones "that have been hacked and those that will be"[401]. Therefore, it is evident that governments and law enforcement need a strategy to counter cybercrime and, with it, CaaS.

This section is not only applicable to Switzerland, but it is instead a global phenomenon. As it was possible to see the current situation in Switzerland through the interview with Mr. Günal Rütsche, the head of the Cyber Department of the Zurich Cantonal Police, Switzerland's situation will be included.

---

391 ASSMAN; BKA (2021), 13.
392 ASSMAN.
393 Ibid.
394 HUANG/SIEGEL/MADNICK, 1.
395 JOHNSEN, 3; MICROSOFT, 8.
396 UNODC (What is it?).
397 GÜNAL RÜTSCHE, Question 23.
398 Ibid.
399 Ibid.
400 KONRADT/SCHILLING/WERNERS, 1.
401 HUANG/SIEGEL/MADNICK, 1.

6.1. Combatting Cybercrime-as-a-Service

There are various ways to counteract CaaS. This chapter will focus on international cooperation, prevention, and the taking down of marketplaces.

As mentioned above, only a few cybercriminals are capable of offering CaaS.[402] It has been observed that the same service is sometimes sold on various marketplaces.[403] The seller often even uses the same nickname.[404] If law enforcement were to succeed in eliminating these few, the market for CaaS would lose in sophistication, and fewer services could be offered.[405] It must be remembered that due to the anonymity in the underground market, identifying individuals is not an easy task.[406]

6.1.1. International Cooperation

According to Mr. Günal Rütsche, the Swiss Police are already targeting the criminals together with other countries.[407] Currently, there are boundaries in existence for law enforcement which are non-existent for cybercriminals.[408] Therefore, international cooperation needs to be more efficient.[409] Extradition and exchanging information work well in some countries, such as Austria.[410] When it comes to Russia, for example, they seldom cooperate as they tolerate any cybercriminal activities as long as they do not attack Russian infrastructure.[411] The difference appears to be the well or ill-functioning of the rule of law in a particular country.[412] Cybercriminals know how long it takes until the Swiss Police gain intelligence from another country, and they deliberately exploit that.[413] International cooperation is also vital as every perpetrator sooner or later makes a mistake, and that is the moment when one

---

[402] JOHNSEN, 104.
[403] JOHNSEN, 50.
[404] Ibid.
[405] JOHNSEN, 50; JOHNSEN/FRANKE, 1.
[406] JOHNSEN/FRANKE, 1.
[407] GÜNAL RÜTSCHE, Question 15.
[408] Ibid.
[409] GÜNAL RÜTSCHE, Question 17; MEYWIRTH, 360.
[410] GÜNAL RÜTSCHE, Question 18.
[411] GÜNAL RÜTSCHE, Question 18; MAURER.
[412] GÜNAL RÜTSCHE, Question 18.
[413] GÜNAL RÜTSCHE, Question 17.

can be identified.[414] The same groups also use the same modus operandi again, which can help when negotiating or identifying them.[415]

There is currently a new convention being negotiated, which is supposed to "promote, facilitate and strengthen international cooperation in preventing" cybercrimes according to Article 1(b) of the UN Cybercrime Convention.[416] It has yet to enter into force.[417]

6.1.2. Prevention

The prevention of CaaS, in general, is better than repression, as more can be done beforehand.[418] According to HUBER, prevention should include three aims:[419]

(1) Awareness must be created.[420] Humans are the weakest link in cyberspace.[421] They need to be sensitised to the threats that lurk in the online world.[422] This is where a criminological theory comes into play: the Routine Activity Theory.[423] This theory states that for a crime, three prerequisites need to be given: (a) a criminal with such an intention, (b) a suitable victim, and (c) the absence of a capable guardian.[424] A victim becomes uninteresting if it is too well educated on the matter of cybercrime.[425] This results in fewer possibilities for the cybercriminals to land a successful attack.[426] Therefore, educating the broad population and raising awareness is highly important.[427]

(2) Technical prevention should intercept fraudulent messages and create security.[428] As the tools used in any CaaS attack are based on the vulnerabilities

---

414 GÜNAL RÜTSCHE, Question 5.
415 Ibid.
416 Draft text of the Convention (A/AC.291/22).
417 UNODC (Sessions).
418 GÜNAL RÜTSCHE, Question 28.
419 HUBER, 87.
420 Ibid.
421 Ibid.
422 HUBER, 87; UNODC (Preventing and Countering).
423 GÜNAL RÜTSCHE, Question 28.
424 HUBER, 71.
425 HUBER, 72.
426 Ibid.
427 UNODC (Preventing and Countering).
428 HUBER, 91.

of a system, companies need to improve their technical knowledge.[429] It is unrealistic to assume that systems like antivirus software could provide 100% security, but it does help to reduce attack possibilities.[430]

(3) The law needs to be able to capture cybercrime trends.[431] Existing laws should regularly be updated to encompass all threats and to capture new and evolving trends.[432] To protect against these trends, security companies need to adapt and react to those trends in order to protect individual people.[433] Companies, in general, need to update their cybersecurity infrastructure.[434] All these security providers need attacked companies to share their findings to further everyone's knowledge.[435] Law enforcement should also be involved in the process of legislating as they need effective tools to pursue cybercrimes.[436]

6.1.3. Taking Down of Marketplaces

Another angle that should have high priority is the taking down of underground marketplaces.[437] If the cybercriminals are constantly disrupted, they will eventually halt their activities.[438] If law enforcement agents gain access to such platforms, it will disturb the trust the cybercriminals put in each other and into the marketplaces.[439] As stated above, trust is essential in the cybercrime economy.[440] The effect on the whole situation may not be significant, but it does have an impact.[441]

6.2. Combatting Cybercrime

It is needless to say that CaaS cannot be combatted alone. There needs to be a strategy for cybercrime as a whole.

---

[429] AN/KIM, 22650.
[430] HUBER, 92.
[431] AN/KIM, 22650; GÜNAL RÜTSCHE, Question 24; HUBER, 93.
[432] AN/KIM, 22650.
[433] Ibid.
[434] Ibid.
[435] KIM/KIM, 674.
[436] GÜNAL RÜTSCHE, Question 24.
[437] BKA (2022), 9.
[438] GÜNAL RÜTSCHE, Question 30.
[439] UNODC (Preventing and Countering).
[440] EUROPOL (2014), 20; UNODC (Criminal Groups engaging in Cyber Organized Crime).
[441] GÜNAL RÜTSCHE, Question 30.

As traces on the internet are fleeting and perpetrators quickly adapt to changes in cybersecurity, cybersecurity companies, attacked companies, and law enforcement agencies need to work together to capture as many of those traces as possible.[442]

To combat cybercrime effectively it has been suggested that cyberspace needs to be viewed as critical infrastructure.[443] The more that is known about cyberspace and cybercrime, the more it is possible to fight against it.[444] If there is an understanding of the underground economy and its trends, it is possible to catch up with upcoming trends quicker and, in turn, protect against related attacks.[445] Therefore, research should be done in that area.[446]

The law enforcement agencies are the ones combatting CaaS and cybercrime.[447] Therefore, they need effective tools to do so.[448] In an environment where time is no longer measured in hours and days but milliseconds, law enforcement must be flexible and quick to adapt.[449] Old-fashioned practices will hinder investigations as they are slow and impractical.[450] The digital competencies of the law enforcement agents need to be improved.[451] The people who are already specialised should be motivated to work for law enforcement.[452] This will be a challenging task as it is assumed that there will be a shortage of skilled people in that area.[453]

The cooperation between research, cybersecurity companies, and law enforcement is paramount.[454] This is the most promising tool to combat cybercrime as they have different competencies.[455]

---

[442] BKA (2021), 30; BKA (2022), 29.
[443] SINN/IDEN, 70.
[444] AN/KIM, 22650.
[445] HUANG/SIEGEL/MADNICK, 2; SOOD/ENBODY, 36.
[446] HUANG/SIEGEL/MADNICK, 2.
[447] BKA (2020), 30; SINN/IDEN, 70.
[448] Ibid.
[449] BKA (2021), 38; GRECO/GRECO, 31; JIROVSKÝ et al., 2.
[450] JIROVSKÝ et al., 2.
[451] BUNDESRAT, 13; GÜNAL RÜTSCHE, Question 24; MEYWIRTH, 360.
[452] GÜNAL RÜTSCHE, Question 24.
[453] EDER (2022).
[454] AN/KIM, 22650. GÜNAL RÜTSCHE, Question 19.
[455] GÜNAL RÜTSCHE, Question 19.

7. Conclusion

To conclude, it can be said that the Cybercrime-as-a-Service business model poses a significant and growing threat to governments, companies, and individuals worldwide. CaaS enables cybercrime on a massive scale by lowering technical barriers and providing a broad spectrum of specialized services to unskilled hackers. As it is now available to a wide range of people, it has fuelled a significant rise in cybercrime. This rise in cybercrime cases has also been made possible through the changing landscape of technology usage. As more people use devices connected to the internet, the number of potential victims has also increased massively. The increase in cases results in more data leaked to the black market and rapidly expanding costs for counteracting and damages due to cybercrimes.

The project has shown the concept behind the CaaS business model and the connections between the perpetrators. The CaaS economy includes a range of specialized services, from malware development and distribution to bulletproof hosting and proxy providers to automated marketplaces selling compromised data and access. It provides the whole value chain of a cyberattack. The cybercrime underground has evolved into a highly organised system where the collaboration of perpetrators leads to a division of labour and increasing specialisation. This specialisation results in more sophisticated attacks, meaning the countermeasures must also be refined.

The growth of CaaS has been made possible through various factors and developments. With the emergence of the dark web and its marketplaces, engaging in physical contact, whether with the seller or the victim, is no longer necessary. Monetary gains through cybercrime have increased drastically with the emergence of CaaS. The increasing sophistication of cybersecurity measures has demanded a higher skill set of perpetrators. Cryptocurrencies have facilitated money laundering and transactions. A perpetrator also has the possibility of working freelance as he is not usually integrated into an organised crime group in the traditional sense. All these reasons have increased the demand for and the offer of cybercrime tools, and it can only be assumed that they will both continue to grow further in the future.

For Organised Crime, there are new opportunities as a result of CaaS. They can now work together globally and commit crimes all over the world. The

evolution of some traditional organised crime groups has been presented, and it has been shown that they use these new possibilities to further their illegal activities. New organised criminal groups are forming, offering all types of cybercrime-related services.

The threats posed by CaaS have been shown to be multifaceted. Some of them can have far-reaching consequences for entire populations. Governments are challenged to find solutions to protect critical infrastructure and sensitive data. Jurisdictional issues also hinder investigations and prosecutions of all cybercrimes. Companies are faced with the possibility of CaaS-enabled large-scale data breaches, ransomware attacks, or other malicious activities that can impair operations and cause financial and reputational damage. Individuals have lost a lot of money through various scams and will continue to do so if there are no feasible countermeasures.

Some strategies to counteract CaaS and cybercrime have been identified and discussed. A multi-angled approach is required to combat the CaaS threat effectively, including strengthening cybersecurity defences, disrupting underground markets, enhancing international law enforcement cooperation, and increasing law enforcement competencies. Staying vigilant and understanding the evolving CaaS landscape is crucial for protecting against these growing cybercrime risks. Individual people need to be educated to spot fraudulent messages and become uninteresting as a target. The fewer people pose as possible victims, the less attractive a cyberattack will be. To combat CaaS and cybercrime law enforcement and cybersecurity providers need the same level of professionalism and collaboration as the perpetrators already have.

"Cybercrime-as-a-Service is still in its infancy"[456], therefore, the future will bring many new challenges concerning this topic. Governments, companies, and individuals must have the tools to counteract this new phenomenon.

[456] GÜNAL RÜTSCHE, Question 10.

8. Further related Questions

An essential aspect in the areas of cybercrime and CaaS is the legal framework on this topic. The UN Cybercrime Convention could be analysed regarding CaaS. Also, the national framework could be studied. The legal possibilities for law enforcement and the methods to recruit skilled people will be essential aspects of such legislation.

The cybercrime underground is highly professional and organised. To counteract CaaS and cybercrime in general, the "good" side needs the same level of professionalism. It needs to be analysed to see if the opposing side, which means cybersecurity companies, law enforcement, and similar, are able to counter the attacks and threats or if there are deficiencies.

Cyberattacks could penetrate new parts of everyday life. With the growing trend of connecting daily life to the internet, Smart Houses and cars, for example, are increasingly at risk of a cyberattack. How they can be protected and what consequences this could have on modern societies could be analysed.

Summary

The text provides an in-depth analysis of the "Cybercrime-as-a-Service" (CaaS) business model and the threats it poses. CaaS has emerged as a significant factor in the rise in cybercrime, making it accessible to many perpetrators. The paper outlines the whole value chain along its nine pillars and the various components of the CaaS business model.

The analysis highlights the diverse range of victims CaaS targets, including governments, companies, and individuals. The paper explores the reasons behind the rapid growth of CaaS, attributing it to the anonymity and financial incentives provided by the internet and the low costs for perpetrators compared to the potential rewards. The text also examines the effects of CaaS on traditional organised crime groups, noting how it has enabled the emergence of more agile, decentralized cybercriminal networks.

The final sections of the paper discuss strategies for combating the threats posed by CaaS to disrupt the CaaS business model itself and enhance overall cybersecurity measures. This project provides a comprehensive and insightful analysis of the CaaS phenomenon and its significant challenges to governments, businesses, and individuals worldwide.

Acknowledgement

I would like to express my gratitude to everyone who took the time to read through my paper and help me improve it as much as possible. Additionally, I want to thank Mr. Serdar Günal Rütsche who has taken the time to answer all my questions. Special thanks go to my two supervisors, Prof. Dr. iur. Gian Ege and MLaw Gishok Kiritharan. Thank you for your valuable input and for organising the very engaging seminar held in February.

List of Sources

1. Literature Sources

AKYAZI UGUR/VAN EETEN MICHEL /GAÑÁN CARLOS H., Measuring Cybercrime as a Service (CaaS) Offerings in a Cybercrime Forum, in: Workshop on the Economics of Information Security (2021), 1–14.
Cited as: "AKYAZI/VAN EETEN/GAÑÁN, …"

ALKHALIL ZAINAB/HEWAGE CHAMINDA/NAWAF LIQAA/KHAN IMTIAZ, Phishing Attacks: A Recent Comprehensive Study and a New Anatomy, Frontiers in Computer Science 3 (2021), 1–23.
Cited as: "ALKHALIL et al., …"

ALRZINI JOMA/PENNINGTON DIANE, A Review of Polymorphic Malware Detection Techniques, International Journal of Advanced Research in Engineering and Technology 11 (2020), 1238–1247.
Cited as: "ALRZINI/PENNINGTON, …"

AN JUNGKOOK/KIM HEE-WOONG, A Data Analytics Approach to the Cybercrime Underground Economy, IEEE Access 6 (2018), 26636–26652.
Cited as: "AN/KIM, …"

BHARDWAJ AANSHI/MANGAT VEENU/VIG RENU/HALDER SUBIR/CONTI MAURO, Distributed Denial of Service Attacks in Cloud: State-of-the-Art of scientific and commercial Solutions, Computer Science Review 39 (2021), 1–28.
Cited as: "BHARDWAJ et al., …"

BRODOWSKI DOMINIK, Transnational Organised Crime and Cybercrime, in: Hauck Pierre/Peterke Sven (Eds.), International Law and Transnational Organised Crime, Oxford 2016, 334–358.
Cited as: "BRODOWSKI, …"

BUNDESAMT FÜR STATISTIK, Polizeiliche Kriminalstatistik: Jahresbericht 2021 der polizeilich registrierten Straftaten, Neuchâtel 2022.
Cited as: "BFS (2021), …"

Id., Polizeiliche Kriminalstatistik: Jahresbericht 2022 der polizeilich registrierten Straftaten, Neuchâtel 2023.

Cited as: "BFS (2022), …"

Id., Polizeiliche Kriminalstatistik: Jahresbericht 2023 der polizeilich registrierten Straftaten, Neuchâtel 2024.
Cited as: "BFS (2023a), …"

BUNDESKRIMINALAMT, Cybercrime, Bundeslagebild 2020, Wiesbaden 2021.
Cited as: "BKA (2020), …"

Id., Cybercrime, Bundeslagebild 2021, Wiesbaden 2022.
Cited as: "BKA (2021), …"

Id., Cybercrime, Bundeslagebild 2022, Wiesbaden 2023.
Cited as: "BKA (2022), …"

BUNDESRAT, Nationale Strategie zum Schutz der Schweiz vor Cyber-Risiken (NCS) 2018-2022, Bern 2018.
Cited as: "BUNDESRAT, …"

CHAINALYSIS, The 2024 Crypto Crime Report: The latest trends in ransomware, scams, hacking and more, New York 2024.
Cited as: "CHAINALYSIS, …"

CHAUDHRY JUNAID A./CHAUDHRY SHAFIQUE A./RITTENHOUSE ROBERT G., Phishing Attacks and Defenses, IJSIA 10 (2016), 247–256.
Cited as: "CHAUDHRY/CHAUDHRY/RITTENHOUSE, …"

ELBAZ CLÉMENT/RILLING LOUIS/MORIN CHRISTINE, Fighting N-Day Vulnerabilities with automated CVSS Vector Prediction at Disclosure, in: ACM International Conference Proceeding Series (2020), 1–10.
Cited as: "ELBAZ/RILLING/MORIN, …"

ESOIMEME EHI E., Identifying and Reducing the Money Laundering Risks posed by Individuals who have been unknowingly recruited as Money Mules, JMLC 24 (2021), 201–212.
Cited as: "ESOIMEME, …"

EUROPEAN UNION AGENCY FOR CYBERSECURITY, Threat Landscape 2020: Main Incidents in the EU and Worldwide, Attiki 2020.
Cited as: "ENISA (2020a), …"

Id., Threat Landscape 2020: Phishing, Attiki 2020.
Cited as: "ENISA (2020b), …"

EUROPEAN UNION AGENCY FOR LAW ENFORCEMENT COOPERATION, Cryptocurrencies: Tracing the Evolution of Criminal Finances, Luxembourg 2021.
Cited as: "EUROPOL (2021c), …"

Id., Cyber-Attacks: The Apex of Crime as a Service, Luxembourg 2023.
Cited as: "EUROPOL (2023b), …"

Id., European Union Serious and Organised Crime Threat Assessment 2021, Luxembourg 2021.
Cited as: "EUROPOL (2021b), …"

Id., Exploring tomorrow's Organised Crime, Luxembourg 2015.
Cited as: "EUROPOL (2015), …"

Id., Internet Organised Crime Threat Assessment 2014, Luxembourg 2014.
Cited as: "EUROPOL (2014), …"

Id., Internet Organised Crime Threat Assessment 2016, Luxembourg 2016.
Cited as: "EUROPOL (2016), …"

Id., Internet Organised Crime Threat Assessment 2017, Luxembourg 2017.
Cited as: "EUROPOL (2017), …"

Id., Internet Organised Crime Threat Assessment 2018, Luxembourg 2018.
Cited as: "EUROPOL (2018), …"

Id., Internet Organised Crime Threat Assessment 2019, Luxembourg 2019.
Cited as: "EUROPOL (2019), …"

Id., Internet Organised Crime Threat Assessment 2021, Luxembourg 2021.
Cited as: "EUROPOL (2021a), …"

Id., Internet Organised Crime Threat Assessment 2023, Luxembourg 2023.
Cited as: "EUROPOL (2023a), …"

FAIRMAN DAVID, The Illegal Economy and Crime as a Service, ITNOW 63 (2021), 14–15.
Cited as: "FAIRMAN, …"

FEDERAL BUREAU OF INVESTIGATION, Internet Crime Report 2023, San Francisco 2024.
Cited as: "FBI, …"

GRECO FULVIO/GRECO GIANPIERO, Organised Crime: Underground Economy and Regulations to combat Cybercrime, EJPSS 4 (2020), 26-39.
Cited as: "GRECO/GRECO, …"

HOQUE NAZRUL/BHATTACHARYYA DHRUBA K./KALITA JUGAL K., Botnet in DDoS Attacks: Trends and Challenges, IEEE Communications Surveys and Tutorials 17 (2015), 2242–2270.
Cited as: "HOQUE/BHATTACHARYYA/KALITA, …"

HUANG KEMAN/SIEGEL MICHAEL/MADNICK STUART, Systematically understanding the Cyber Attack Business: A Survey, ACM Computing Surveys 51 (2019), 1–36.
Cited as: "HUANG/SIEGEL/MADNICK, …"

HUBER EDITH, Cybercrime: Eine Einführung, Wiesbaden 2019.
Cited as: "HUBER, …"

HYSLIP THOMAS S., Cybercrime-as-a-Service Operations, in: Holt Thomas J./Bossler Adam M. (Eds.), The Palgrave Handbook of International Cybercrime and Cyberdeviance, Cham 2020, 815–846.
Cited as: "HYSLIP, …"

JIROVSKÝ VÁCLAV/PASTOREK ANDREJ/MÜHLHÄUSER MAX/TUNDIS ANDREA, Cybercrime and Organized Crime, in: Proceedings of the 13th International Conference on Availability, Reliability and Security (2018), ACM (2018), 1–5.
Cited as: "JIROVSKÝ et al., …"

JOHNSEN JAN WILLIAM, Interdisciplinary Approach to Criminal Network Analysis: Opportunities and Challenges, Doctoral Thesis, Gjøvik 2022.
Cited as: "JOHNSEN, …"

JOHNSEN JAN WILLIAM/FRANKE KATRIN, Identifying proficient Cybercriminals through Text and Network Analysis, in: IEEE International Conference on Intelligence and Security Informatics (2020), 1–7.
Cited as: "JOHNSEN/FRANKE, …"

KAUR SHUBHDEEP/RANDHAWA SUKHCHANDAN, Dark Web: A Web of Crimes, Wireless Personal Communications 112 (2020), 2131–2158.
Cited as: "KAUR/RANDHAWA, …"

KIM SEUNG H./KIM BYUNG C., Differential Effects of Prior Experience on the Malware Resolution Process, MISQ 38 (2014), 655–678.
Cited as: "KIM/KIM, …)

KONRADT CHRISTIAN/SCHILLING ANDREAS/WERNERS BRIGITTE, Phishing: An economic Analysis of Cybercrime Perpetrators, Computers & Security 58 (2016), 39–46.
Cited as: "KONRADT/SCHILLING/WERNERS, …"

LASTDRAGER ELMER E., Achieving a consensual Definition of Phishing based on a systematic Review of the Literature, Crime Science 3 (2014), 1–10.
Cited as: "LASTDRAGER, …"

LAVORGNA ANITA, Organized Crime and Cybercrime, in: Holt Thomas J./Bossler Adam M. (Eds.), The Palgrave Handbook of International Cybercrime and Cyberdeviance, Cham 2020, 117–134.
Cited as: "LAVORGNA, …"

LEUKFELDT ERIC R./LAVORGNA ANITA/KLEEMANS EDWARD R., Organised Cybercrime or Cybercrime that is Organised? An Assessment of the Conceptualisation of Financial Cybercrime as Organised Crime, European Journal on Criminal Policy and Research 23 (2017), 287–300.
Cited as: "LEUKFELDT/LAVORGNA/KLEEMANS, …"

LEUKFELDT ERIC R./NOTTÉ RAOUL J. /MALSCH MARIJKE, Exploring the Needs of Victims of cyber-dependent and cyber-enabled Crimes, Victims & Offenders 15 (2020), 60–77.
Cited as: "LEUKFELDT/NOTTÉ/MALSCH, …"

LIGGETT ROBERTA/LEE JIN R./RODDY ARIEL L./WALLIN MIKAELA A., The Dark Web as a Platform for Crime: An Exploration of illicit Drug, Firearm, CSAM, and Cybercrime Markets, in: Holt Thomas J./Bossler Adam M. (Eds.), The Palgrave Handbook of International Cybercrime and Cyberdeviance, Cham 2020, 91–116.

Cited as: "LIGGETT et al., …"

LUSTHAUS JONATHAN, Industry of Anonymity: Inside the Business of Cybercrime, Cambridge, Massachusetts 2018.
Cited as: "LUSTHAUS, …"

MANKY DEREK, Cybercrime as a Service: A very modern Business, Computer Fraud & Security (2013), 9–13.
Cited as: "MANKY, …"

MANSKE MIRKO, Crime-as-a-Service: Die neun Säulen - Eine Phänomenbeschreibung, Kriminalistik 74 (2020), 235–239.
Cited as: "MANSKE, …"

MARKWALDER NORA, Wandel der Kriminalität in den letzten 20 Jahren: Von offline zu online?, in: Schwarzenegger Christian/Nägeli Rolf/Europa Institut an der Universität Zürich (Eds.), Schwachstelle Mensch: Prävention gegen alte und neue Formen der Kriminalität - 12. Zürcher Präventionsforum – Tagungsband 2021, Zürich 2021.
Cited as: "MARKWALDER, …"

MEYWIRTH CARSTEN, Crime-as-a-Service: Die kriminelle Cloud verändert das Kriminalitätsgeschehen, Kriminalistik 70 (2016), 355–360.
Cited as: "MEYWIRTH, …"

MICROSOFT, Microsoft Digital Defense Report, Redmond 2021.
Cited as: "MICROSOFT, …"

MINAKAWA MAKOTO, Defining Transnational Organised Crime in International Law, Nagoya Gakuin University Review, Social Sciences 1 and 2 (2023), 225–236.
Cited as: "MINAKAWA, …"

MOYA EVA/LANUZA LETICIA, Crime-as-a-Service: Inteligencia Competitiva en el Lado Cibercriminal para la Era Post-Covid19, Business Intelligence 3 (2021), 25–34.
Cited as: "MOYA/LANUZA, …"

NAZAH SAIBA/HUDA SHAMSUL/ABAWAJY JEMAL/HASSAN MOHAMMAD M., Evolution of Dark Web Threat Analysis and Detection: A systematic Approach, IEEE Access 8 (2020), 171796–171819.

Cited as: "NAZAH et al., …"

PAQUET-CLOUSTON MASARAH/HASLHOFER BERNHARD/DUPONT BENOÎT, Ransomware payments in the Bitcoin ecosystem, Journal of Cybersecurity 5 (2019), 1–11.
Cited as: "PAQUET-CLOUSTON/HASLHOFER/DUPONT, …"

RAZAK MOHD FAIZAL AB/ANUAR NOR BADRUL/SALLEH ROSLI/FIRDAUS AHMAD, The Rise of "Malware": Bibliometric Analysis of Malware Study, Journal of Network and Computer Applications 75 (2016), 58–76.
Cited as: "RAZAK et al., …"

REID ALAN S., Financial Crime in the Twenty-First Century: The Rise of the Virtual Collar Criminal, in: Ryder, Nic (Ed.), White Collar Crime and Risk, London 2018, 231–251.
Cited as: "REID, …"

RESHMI T. R., Information Security Breaches due to Ransomware Attacks: A systematic Literature Review, International Journal of Information Management Data Insights 1 (2021), 1-10.
Cited as: "RESHIMI, …"

SALAHDINE FATIMA/KAABOUCH NAIMA, Social Engineering Attacks: A Survey, Future Internet 11 (2019), 1–17.
Cited as: "SALAHDINE/KAABOUCH, …"

SINN ARNDT/BOJEN LARS/DENNHARDT YARI/IDEN MARCEL P./PÖRTNER PATRICK, Organisierte Kriminalität? Frag doch einfach! Klare Antworten aus erster Hand, München 2023.
Cited as: "SINN et al., …"

SINN ARNDT/IDEN MARCEL, Alte und neue Bedrohungen der Organisierten Kriminalität, SIAK-Journal − Zeitschrift für Polizeiwissenschaft und polizeiliche Praxis 1 (2023), 62–72.
Cited as: "SINN/IDEN, …"

SOOD ADITYA K./ENBODY RICHARD J., Crimeware-as-a-Service: A Survey of commoditized Crimeware in the Underground Market, International Journal of Critical Infrastructure Protection 6 (2013), 28–38.

Cited as: "SOOD/ENBODY, …"

SUNDE INGER M., A new Thing under the Sun? Crime in the Digitized Society, in: Nordisk Samarbejdsråd for Kriminologi's 58. Research Seminar: New Challenges in Criminology: Can old Theories be used to explain or understand new Crimes? (2016), 60–79.
Cited as: "SUNDE, …"

UNITED NATIONS OFFICE ON DRUGS AND CRIME, Comprehensive Study on Cybercrime - Draft, Vienna 2013.
Cited as: "UNODC (2013), …"

WAINWRIGHT ROBERT/CILLUFFO FRANK J., Responding to Cybercrime at Scale: Operation Avalanche — A Case Study, Auburn 2017.
Cited as: "WAINWRIGHT/CILLUFFO, …"

WICKER STEPHEN B., The Ethics of Zero-Day Exploits: The NSA meets the Trolley Car, Communications of the ACM 64 (2021), 97–103.
Cited as: "WICKER, …"

2. Internet Sources

ASSMAN BRILL, Discover the Risks of Crime-as-a-Service (CaaS) for Businesses, Convergence Networks, <https://convergencenetworks.com/blog/crime-as-a-service-a-growing-risk-for-businesses-in-the-digital-age/> (visited last 10 December 2023).
Cited as: "ASSMAN."

BRITISH BROADCAST CORPORATION, Cyber-attack: US and UK blame North Korea for WannaCry, <https://www.bbc.com/news/world-us-canada-42407488> (visited last 16 April 2024).
Cited as: "BBC."

BOSTON CONSULTING GROUP, Unveiling the Shadow Economy, <https://www.bcg.com/publications/2023/unveiling-the-shadow-economy> (visited last 26 March 2024).
Cited as: "Boston Consulting Group."

BUNDESAMT FÜR STATISTIK, Benutzte Geräte, <https://www.bfs.admin.ch/bfs/de/home/statistiken/kultur-medien-informationsgesellschaft-sport/informationsgesellschaft/gesamtindikatoren/haushalte-bevoelkerung/mobile-internetnutzung.html> (visited last 7 April 2024).
Cited as: "BFS (2023b)."

BUNDESKRIMINALAMT, Cybercrime, <https://www.bka.de/DE/DasBKA/OrganisationAufbau/Fachabteilungen/Cybercrime/cybercrime_node.html> (visited last 26 March 2024).
Cited as: "BKA (Cybercrime)."

DRÖSSER CHRISTOPH, US-Wahl 2016: «Der Einfluss der russischen Tweets war, wenn überhaupt, begrenzt», Die Zeit, <https://www.zeit.de/digital/internet/2023-01/us-wahl-2016-donald-trump-russland-einfluss-twitter-trolle> (visited last 23 April 2024).
Cited as: "DRÖSSER."

EDER TANJA, Fachkräftemangel: IT-Stellen bleiben unbesetzt, SRF, <https://www.srf.ch/news/wirtschaft/fachkraeftemangel-it-stellen-bleiben-unbesetzt> (visited last 8 December 2023).
Cited as: "EDER (2022)."

Id., Nordkorea: Krypto-Diebstahl für Raketenprogramm, SRF, <https://www.srf.ch/news/inter-national/ein-staat-klaut-krypto-nordkoreas-raketen-fliegen-dank-kryptowaehrungen> (visited last 5 April 2024).
Cited as: "EDER (2024)."

EDMONDSON JAMES, Crime As A Service: Understanding the latest Threat on the Dark Web, BusinessTechWeekly, <https://www.businesstechweekly.com/cybersecurity/risk-management/crime-as-a-service/> (visited last 27 March 2024).
Cited as: "EDMONDSON."

EIDGENÖSSISCHES FINANZDEPARTEMENT EFD, Hackerangriff auf die Firma Concevis: Auch die Bundesverwaltung ist betroffen, <https://www.admin.ch/gov/de/start/doku-

mentation/medienmitteilungen.msg-id-98595.html> (visited last 11 December 2023).
Cited as: "EFD."

EUROPEAN UNION AGENCY FOR LAW ENFORCEMENT COOPERATION, Money Muling, <https://www.europol.europa.eu/operations-services-and-innovation/public-awareness-and-prevention-guides/money-muling> (visited last 23 April 2024).
Cited as: "EUROPOL (Money Muling)."

GRIFFITHS CHARLES, The Latest Phishing Statistics, AAG IT, <https://aag-it.com/the-latest-phishing-statistics/> (visited last 29 March 2024).
Cited as: "GRIFFITHS."

HASSO-PLATTNER-INSTITUT, Identity Leak Checker, <https://sec.hpi.de/ilc/statistics> (visited last 3 April 2024).
Cited as: "HASSO-PLATTNER-INSTITUT."

HONG KONG COMPUTER EMERGENCY RESPONSE TEAM COORDINATION CENTRE, Unmasking Cybercrime-as-a-Service: The Dark Side of Digital Convenience, <https://www.hkcert.org/blog/unmasking-cybercrime-as-a-service-the-dark-side-of-digital-convenience> (visited last 2 February 2024).
Cited as: "HONG KONG COMPUTER EMERGENCY RESPONSE TEAM COORDINATION CENTRE."

JABBER.ORG, <https://www.jabber.org/> (visited 27 March 2024).
Cited as: "JABBER."

KAPKO MATT, Prospect Medical stolen Data listed for Sale by emerging Ransomware Group, Cybersecurity Dive, <https://www.cybersecurity dive.com/news/prospect-medical-data-stolen/691945/> (visited last 23 April 2024).
Cited as: "KAPKO."

KESSLER GLENN, The Truth about Russia, Trump and the 2016 Election, The Washington Post, <https://www.washingtonpost.com/politics/2023/05/17/truth-about-russia-trump-2016-election/> (visited last 23 April 2024).
Cited as: "KESSLER."

MAURER TIM, Why the Russian Government turns a blind Eye to Cybercriminals, Carnegie Endowment for International Peace, <https://carnegieendowment.org/2018/02/02/why-russian-government-turns-blind-eye-to-cybercriminals-pub-75499> (visited last 24 April 2024).
Cited as: "MAURER."

MEIJER BART H./SIEBOLD SABINE, «Pro-Russia» Hackers down EU Parliament Website for Hours, Reuters, <https://www.reuters.com/world/europe/pro-kremlin-group-says-responsible-cyberattack-eu-parliament-official-2022-11-23/> (visited last 5 April 2024).
Cited as: "MEIJER/SIEBOLD."

MORGAN STEVE, Cybercrime to cost the World $10.5 Trillion annually by 2025, Cybersecurity Ventures, <https://cybersecurityventures.com/cybercrime-damages-6-trillion-by-2021/> (visited last 4 February 2024).
Cited as: "MORGAN."

NATIONAL CYBER SECURITY CENTER, SVR Cyber Actors adapt Tactics for initial Cloud Access, <https://www.ncsc.gov.uk/news/svr-cyber-actors-adapt-tactics-for-initial-cloud-access> (visited last 5 April 2024).
Cited as: "NATIONAL CYBER SECURITY CENTER."

NEUE ZÜRCHER ZEITUNG, US-Geheimdienste: Russland pumpte viel Geld in Wahleinmischungen, NZZ <https://www.nzz.ch/international/us-geheimdienste-russland-pumpte-viel-geld-in-wahleinmischungen-ld.1702656> (visited last 23 April 2024).
Cited as: "NZZ."

NICHOLS MICHELLE, Exclusive: UN Experts investigate 58 Cyberattacks worth $3 bln by North Korea, Reuters, <https://www.reuters.com/technology/cybersecurity/un-experts-investigate-58-cyberattacks-worth-3-bln-by-north-korea-2024-02-08/> (visited last 5 April 2024).
Cited as: "NICHOLS."

REED JONATHAN, Cyberattacks rise sharply against Governments and Schools, Security Intelligence, <https://securityintelligence.com/news/

cyberattacks-rise-sharply-against-governments-schools/> (visited last 24 April 2024).
Cited as: "REED."

SCHAPPERT STEFANIE, Multi-Hospital Ransom Attack in U.S. claimed by Rhysida Gang, Cybernews, <https://cybernews.com/security/prospect-medical-holdings-ransom-attack-rhysida-gang/> (visited last 23 April 2024).
Cited as: "SCHAPPERT."

UNITED NATIONS OFFICE ON DRUGS AND CRIME, Ad Hoc Committee: Home, <//www.unodc.org/unodc/en/cybercrime/ad_hoc_committee/home> (visited last 25 April 2024).
Cited as: "UNODC (Sessions)."

Id., Organized Crime: Cybercrime Module 13 Key Issues – Conceptualizing Organized Crime and Defining the Actors involved, <https://www.unodc.org/e4j/en/cybercrime/module-13/key-issues/conceptualizing-organized-crime-and-defining-the-actors-involved.html> (visited last 20 April 2024).
Cited as: "UNODC (Actors involved)."

Id., Organized Crime: Cybercrime Module 13 Key Issues – Criminal Groups engaging in Cyber Organized Crime, <https://www.unodc.org/e4j/en/cybercrime/module-13/key-issues/criminal-groups-engaging-in-cyber-organized-crime.html> (visited last 20 April 2024).
Cited as: "UNODC (Criminal Groups engaging in Cyber Organized Crime)."

Id., Organized Crime: Cybercrime Module 13 Key Issues – Cyber Organized Crime: What is it?, <https://www.unodc.org/ e4j/en/cybercrime/module-13/key-issues/cyber-organized-crime_what-is-it.html> (visited last 20 April 2024).
Cited as: "UNODC (What is it?)."

Id., Organized Crime: Cybercrime Module 13 Key Issues – Cyber Organized Crime Activities, <https://www.unodc.org/e4j/en/cybercrime/module-13/key-issues/cyber-organized-crime-activities.html> (visited last 20 April 2024).

Cited as: "UNODC (Cyber Organized Crime Activities)."

Id., Organized Crime: Cybercrime Module 13 Key Issues – Preventing and Countering Cyber Organized Crime, <https://www.unodc.org/e4j/en/cybercrime/module-13/key-issues/preventing-and-countering-cyber-organized-crime.html> (visited last 20 April 2024).
Cited as: "UNODC (Preventing and Countering)."

VOLZ DUSTIN, U.S. blames North Korea for «WannaCry» Cyber Attack, Reuters, <https://www.reuters.com/article/idUSKBN1ED00Q/> (visited last 16 April 2024).
Cited as: "VOLZ."

3. Materials

Draft text of the UN Convention on Countering the Use of Information and Communications Technologies for Criminal Purposes (A/AC.291/22), Status as of 1 September 2023, <https://www.unodc.org/unodc/en/cybercrime/ad_hoc_committee/ahc_sixth_session/main> (visited last 24 April 2024).

Nationale Strategie zum Schutz kritischer Infrastrukturen: Ganzheitlicher Ansatz zur Sicherstellung der Verfügbarkeit von essenziellen Gütern und Dienstleistungen from 16 June 2023.
Cited as: "BBI 2023 1659, …"

UNITED NATION GENERAL ASSEMBLY, Interpretative Notes for the official Records (Travaux Préparatoires) of the Negotiation of the United Nations Convention against Transnational Organized Crime and the Protocols thereto, UN Document A/55/383/Add.1, 2000.
Cited as: "UN GENERAL ASSEMBLY, …"

Annex: Interview with Mr. Serdar Günal Rütsche (Head of Cybercrime at Kantonspolizei Zürich) conducted on 5 April 2024

1. Are the perpetrators individuals who get together occasionally to commit a cyberattack, or are they groups in the sense of an organisation, as we usually know them?

It's clear that no one can carry out a cyberattack like the one we're talking about alone; it has to be a group and it has to be international. Then, it already is a case of Organised Crime. These groups have very different compositions. Some are responsible for one thing, others for another. Rarely or never is someone alone because you can't do it alone. It cannot be ruled out that some people try to do it alone. But they won't be successful. Ultimately, these are groups that divide the work among themselves.

2. If they are organised, are there groups that are structured like a company? Or is it more a case of doing a project together and then going their separate ways again?

Yes, that does exist. These are the so-called affiliates. They work on a project together with a specific ransomware and if it burns up, then the whole thing is put back together again. They also know each other. They don't do any commercial advertising, but they know each other and arrange themselves accordingly. You need a specialist for encryption and a specialist for payment transactions, for example, and they must be able to work together somehow.

3. Your experience is that the people do know each other? In the literature, it is always written that the whole thing is very anonymous. That you have no idea who the other person is.

No, they don't know each other in the sense that you know what someone looks like. But they know who is where. With anonymity, it's perhaps the case that you don't know each other personally. But you know that the user CC248 is the one who can programme ransomware or who can programme good ransomware for Apple. You then obtain this from him.

4. Would that also mean it would be easier for law enforcement authorities to identify an individual?

No, it's not easier at all, whether they know each other or not. The perpetrators will never tell us that they know someone, that it was that person who did it. It doesn't matter if it is anonymous. You will always take the position that you don't know the other person. And if you don't know someone, then you can't make contact with the person, if that's the definition of knowing someone. Then there is also the question of what anonymity is. You can be anonymous, but you can still have a business relationship with someone for two years. It doesn't make it any easier or more difficult.

5. Is it even possible for the prosecution authorities to identify someone, i.e., to know that person XY, a resident in Zurich, was involved in this attack?

You can't solve a single ransomware case when a company is affected. The perpetrators also make fewer mistakes there. But they don't just do it once. They do it several times. If you do it several times, it is quite clear that they are making a mistake. If they make a mistake, and we recognise these mistakes, we are ultimately successful. If you are always completely anonymous and never make mistakes, then it becomes difficult, but there is no such person. There is no such group. In the end, the motivation of the perpetrators is money. They want to get cash and transfer money. They do that again and again. If you do it very often, they follow the same procedure. We call this modus operandi. We compare this modus operandi with this modus operandi: For example, when a company pays, they don't want to negotiate at all, while others want to negotiate. Some encrypt first and then leak. These are different modus operandi. All of this needs to be defined. Then we will also be successful.

6. Is it possible to quantify how many people are involved in a structure or in the entire cybercrime market economy?

No, you can't back that up with facts. There must be more than one person. The number varies greatly depending on the group. We see up to ten people who can be identified in our cases, but I would never call that a standard. We have had cases with up to ten people involved. One person does the phishing, the other does the ransomware, the third has the technical infrastructure, the fourth is there to negotiate, and the last does the translations, for example.

7. In the CaaS business, there is the developer and the perpetrator, who may be technically unskilled. How much money does he end up with? He might have to bear a lot of costs. Can this be quantified?

We know from old cases that it's 80% to 20%. 80% remains with the person who realises it, and 20% stays with the person who did it.

8. Does that mean it's not lucrative for someone who only carries out small attacks?

It depends on the scale on which you do it. If you do it in large quantities, then, of course, it is.

9. For someone who makes 50 Francs once a month.

That's not possible. It wouldn't work, either. It's primarily larger companies, and then it works. That's why it's very attractive there.

10. How do you feel the whole business model could develop in the future?

I think there will be more specialisation, where you really declare that you can buy it as a service. This will then also be expanded with AI (artificial intelligence) or made even more specific. And I think that will undoubtedly grow. After all, Cybercrime-as-a-Service is still in its infancy. Some people have also realised that it can be used for simple blackmail. In the past, you had to have someone do it for you. Today, you can simply order this service. This will probably increase in the future if ordering the service becomes more accessible. Today, it's all more complex. Access to the dark net is not easy.

11. If it is more complex today because of the dark net, does that mean it could develop into the deep web or the open access area?

Yes, but as soon as it enters the public domain, it's already public to everyone, and then it's easier to track. Then, the criminals are no longer interested in it. They don't break into a house where they can see the police standing right in front of it. It has to be in an area where you have a good chance of remaining undetected. You won't be able to buy it on the public web. That won't be possible. Or only for a short time, until it is discovered and then switched off again.

12. Is Cybercrime-as-a-Service more dangerous than analogue supplied crime? Or is it a different phenomenon?

I don't think it's more dangerous. You can already hire someone to do something in the analogue world today. It simply becomes possible for those who don't have the means to access it right now. This will probably mean that there will be more of it. In the past, not everyone could have ransomware. Today you can order it for little money.

13. That would mean it's more the masses that will make the difference?

Yes, exactly. And it's also the availability that will make a difference. If you have it available and then buy it, that's what will make the difference, of course.

14. What are the biggest threats that could arise in connection with CaaS today or in the future?

I believe that the whole ransomware story will continue to be the biggest threat in the future, as will the uncontrolled outflow of data. These are the two very dangerous issues we will have in the future.

15. Do law enforcement agencies have the means to take action specifically against CaaS, or is this something that is dealt with in the whole context of cybercrime?

We take a specific approach based on priorities, primarily against the perpetrators. You can do that if you work together internationally. However, the perpetrators know that crime on the internet differs from crime in the real world in that there are no borders on the internet. In the real world, jurisdiction is the most essential thing in criminal law. Physical borders determine this jurisdiction. These do not exist on the internet. In other words, there is no jurisdiction, so you have to work together, and I think that is the most important weapon.

16. In other words, you create equal opportunities. Since crime has no limits, must law enforcement also have no limits?

Law enforcement always has limits because it is so regulated, and it needs a legal basis, but we need to become more efficient in cooperation.

17. When you say cooperation needs to become more efficient, is it not yet working well?

It doesn't work so well yet because there is a language barrier when you work together internationally. International agreements are needed. When you

communicate with Belgium, for example, it takes time. That is what speaks against the law enforcement authorities. The criminals know that if I request something on the Thursday before Easter, it will already be Tuesday by the time the request for mutual legal assistance is in the U.S. By then, a few million will be gone.

18. Is it easier with some countries, such as Germany, because of the language? Are there countries that don't participate on principle?

The language is not such a problem if you keep it in English. Cooperation works in countries with a functioning legal system. Legal assistance to Russia does not currently work, and most ransomware perpetrators come from Russia. But we can't force the Russians to do so. Legal assistance with Austria works, but it may take a week, not just three hours, as we have in Switzerland between the cantons. Legal assistance to America is very complex. Judges there first have to decide whether anyone in the USA will take any action.

19. It is often said in the literature that cooperation between the police, research, and all cyber security companies is crucial. Do you agree, and if so, how well does this cooperation work?

It is very important because the police, research, and private companies have entirely different competencies. Bringing these competencies together is actually the most important and most promising method. For example, research is investigating how quantum technology can be used, which is now being researched at ETH. Tests can be carried out in the private sector, which is not possible here because we don't have the infrastructure. This collaboration is also working better and better. But it also needs a legal basis. You can't make x terabytes of data available to a private individual so that they can view criminal images. There needs to be some kind of agreement. We're on the right track, and it works in Switzerland. But that is also important.

20. Concerning Organised Crime: If you look at the traditionally organised groups, are they more likely to be customers or providers of CaaS?

No, those who offer it are already organised. The customers are in smaller groups. The organised groups are already the providers.

21. In other words, have the criminal groups operating analogue moved into cyberspace?

Exactly.

22. Do you feel that organised crime has changed in the sense of these traditional groups since CaaS and cybercrime, in general, came into being?

I think there is certainly a shift from property offences to the internet. You can commit fraud from anywhere, pay anonymously with cryptocurrencies, and transfer them. Traditional fraud, as it used to be done, has shifted to the internet. In the past, grandchild scams were committed by calling someone on the phone. That still happens, but nowadays, it's more online investment fraud.

23. Is it justified that a lot of attention is being paid to this issue, or do you think other cybercrime areas require more immediate attention?

You really have to prioritise this. A study from Chainalysis just came out today [05.04.2024]. That's a company that does crypto analyses. In this study, they said that almost USD 1 billion in ransom money was paid via their platform. You have to imagine that: One billion USD via just one platform. You have to pay a lot of attention to that. This means we, as authorities, must be educated thoroughly enough to understand this and see how it happens. It is also essential to sensitise the population so they don't fall for it. The perpetrators do not carry out targeted attacks but random attacks. You become a victim through a random attack, and you become a victim by doing something wrong somewhere at the beginning. So, you've clicked on a phishing e-mail or whatever. You have to train people accordingly.

24. When you say that the authorities need to get fit, what are the most important points that need to be addressed?

The digital skills of employees need to be improved. We need to get hold of specialists who are specialised in this area. We must attract and motivate them to work for the law enforcement agency. I believe that as a law enforcement agency, we always have to work together with politicians to develop a legal basis to work effectively. It's a new environment. That's why there aren't many legal bases, and you have to keep adapting them.

25. When you talk about the legal bases, do you know whether there is an offence, apart from fraud, where CaaS could be included?

Online investment fraud is one where you are led to believe that you can make huge returns within a very short time. This is usually on a website that someone has programmed, where you can see that you are making a return even though everything is shit. Someone else ensures that the money from your account goes into a crypto wallet so you can send it on from there. Someone else converts it into a currency and then cashes it out.

26. The legal bases for criminalising the whole phenomenon are, therefore, given?

They are in place, but there is no cooperation between the police to exchange information. This legal basis must be created.

27. The end product is there, but how to get there is still unclear?

Exactly, that is not yet fully defined.

28. Is there anything on this topic that has not yet been mentioned but would be important to address? Or something you've had experience within your line of work?

I believe we need international cooperation if we want to be strong in the fight against Cybercrime-as-a-Service because it doesn't happen locally. Secondly, we need very good specialists in Switzerland who are trained in this area and can be deployed accordingly. Thirdly, we always need political understanding in order to create the appropriate legal basis in a timely manner. What is also important and can be said in conclusion: I believe that prevention is more important than repression in the fight against Cybercrime-as-a-Service. In other words, you can achieve much more preventively than you can catch up with investigations, i.e., repression afterward. By prevention, I mean educating people. If that doesn't happen, then we end up with the Routine Activity Theory. It says that if we make ourselves unattractive to offenders, they will stop coming to us. We can make ourselves unattractive by training people, training users well, and creating a technical infrastructure that doesn't have these security loopholes.

29. On the perpetrator side, are there preventative measures that could be taken so that a perpetrator doesn't get into an organisation in the first place?

We can do less on the perpetrator side because, as far as we are concerned, there are fewer perpetrators here in Switzerland. So, perpetrator prevention is difficult.

30. Marketplaces are shut down from time to time. Is there any point in shutting down these marketplaces if a new website goes online the next day?

Absolutely. If you don't do anything, then they feel free to do what they want. But if you keep disturbing them, then at some point, they will feel disturbed and stop. That's always useful. It's always a question of whether it's any use washing the car today if I know it will rain tomorrow. It gets clean there, too. What you do also has an immediate effect. It may have a small impact on the whole, but it does have an effect.

Declaration of Plagiarism

I hereby declare that I have prepared this written work independently and only with the help of the sources listed in the lists or the notes. I also declare that I have not used this work elsewhere as proof of performance. The thesis may be checked for plagiarism using appropriate software. I agree that the University of Zurich may commission appropriate service providers in Switzerland or abroad for this purpose, which will be checked by the University to ensure data security.

_____

Bonstetten, 4 May 2024