How to Not Get Away with Cybercrime? The Techniques and Challenges of Cybercrime Investigation

Valeriia Lymishchenko,
LL.B. Higher School of Economics,
LL.M. University of Bologna

Introduction

The active development of the informational technologies in the recent years leads not only to new opportunities, but also to new challenges. In the issue of informatization of society and the state, one of the main problems is cybercrime. In 2021, according to the data of the Federal Bureau of Investigation, only in the United States of America were registered **847,376** cybercrimes[1], which became an unprecedented increase of the cybercrimes the world ever encountered with. In comparison, in 2019, the number of committed cybercrimes were approximately **460,000[2].**

In 2021 if the damage from the cybercrime was measured as a country, then it will be totaling **$6 trillion USD** - would be the world's third-largest economy after the U.S. and China[3]. All this make a cybercrime one of the most dangerous threats in the modern world.

1. What Is a Cybercrime?

The word "cybercrime" originates from greek "kubernetes" (kubernētēs, steer) and latin "crimen" ("judgment") and it is generally understood as a criminal activity committed using the Internet. The common use of this term was started in the 1980-s and for the recent few years raised significantly due both to the technological growth and the increased attention of the public to the cybercrime awareness.

Investigation and research of the cybercrime is a sophisticated multi-level task due to the diversity and complexity of the cybercrime's essence. The Internet touches too many important pieces of a person's everyday life and for that reason it requires a specific expertise of the person conducting a cybercrime investigation.

Through the years of its spreading, cybercrimes have established themselves as a global, multinational problem, affecting the lives of millions of people around the world. Digitalization

[1] FBI. (2021). *The Internet Crime Report*, p. 3.
[2] FBI. (2020). *The Internet Crime Report*, p. 3.
[3] Freeze, D. (2020, November 9). *Global cybercrime damages predicted to reach $6 trillion annually by 2021*. Cybercrime Magazine. Retrieved May 5, 2022, from https://cybersecurityventures.com/annual-cybercrime-report-2020/.

of the world’s economic, social, and financial infrastructure, and even military and ecological ones, carry not only the obvious advantages of the acceleration and simplification of the processes but also makes the holders of these processes’ potential victims of the cybercriminals.

Ironically, the main reason for the continued spread of the cybercrimes are the humans’ actions itself. All the technology associated issues involve the use of data. They even said that “data is the new gold”. But unlike real gold, the data is produced by humanity as-it-is. Everyday millions of people provide their data to the world wide web networks. Our data is sold, bought, and exchanged as the most valuable currency and regrettably, not always in the good hands. This creates numerous possibilities of compromising a person's data and makes cybercrimes such attractive as the easiest way to receive this data.

2. Main Types of Cybercrimes in the Underground Activities

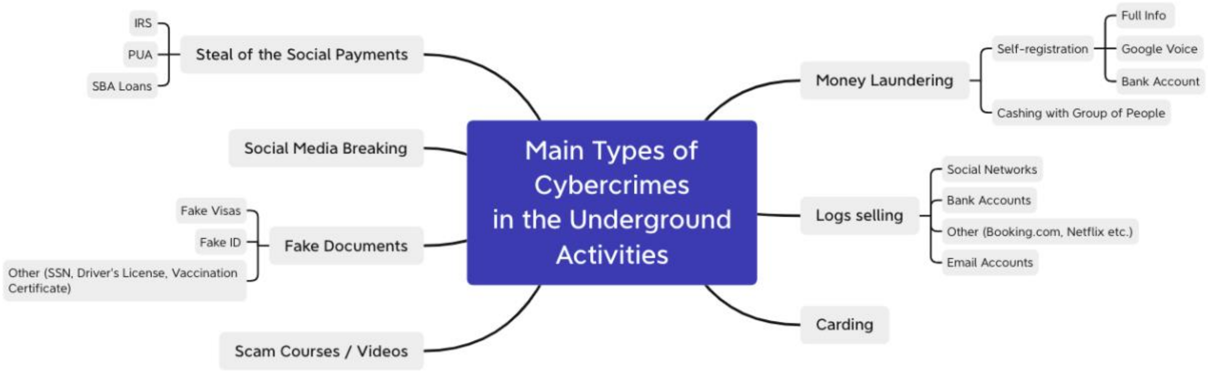
A definition of cybercrime shows that the cybercrime is the crime which happens in the sphere of the Information and Communication Technologies (ICTs), or, in other words, it involves a computer and, accordingly, a network. Altogether, it constitutes the “cyberspace”, which now indicates “the whole sphere of computer networks, cables, transmission protocols and the relevant software necessary to make it work”[4]. One of the most important parts of the cyberspace is a network called “the Internet”, which connects computers all over the world. In the basis of the Internet lies the Internet protocol suite (TCP/IP), which provides end-to-end data communication, based on the network packets, which makes it stable and secure. Inside the Internet there is a vast range of technologies, which also includes the World Wide Web (the WWW).

Basically, the WWW is a system of information in the form of webpages which exists on the base of the Internet and TCP/IP. In general, the WWW can be presented in three main layers: the Surface Web, the Deep Web, and the Dark Web. Usually, it is presented in the form of an iceberg. The Surface Web is the open part of the “iceberg” which consists of the open web pages, whose context is indexed by the standard web search-engines. It is accessible to anybody using the Internet, in contrast with a Deep Web, which is the underwater part, hidden behind close login forms and private data. The Dark Web part is the part of the Deep Web, but is the deepest one, existing in a form of overlay network, which means that it could be accessed only with specific software and configurations. Inside the Dark Web part of the WWW there are encrypted proxy networks, which include, for example, The Onion Router (Tor), the Invisible Internet Project (I2P) and Freenet. Encryption technologies also formed the basis for the messengers like Telegram and

[4] Giacomello, G. & Siroli, G. P. (2016). *War in Cyberspace*, p.4.

Signal. These technologies were created with the goal to support the privacy and censorship resistance movement but also it has a reputation as a platform for illegal activities.

Thus, the Tor became one of the biggest sources of underground forums for people, committing the cybercrimes. It contains multiple pieces of advice for the cybercriminals, manuals on fraud, scamming schemes and provides an opportunity to gain the profit for the illicit activities. Another source which contains multiple hidden channels for cybercriminals communication is Telegram. These activities could be represented in the following way:



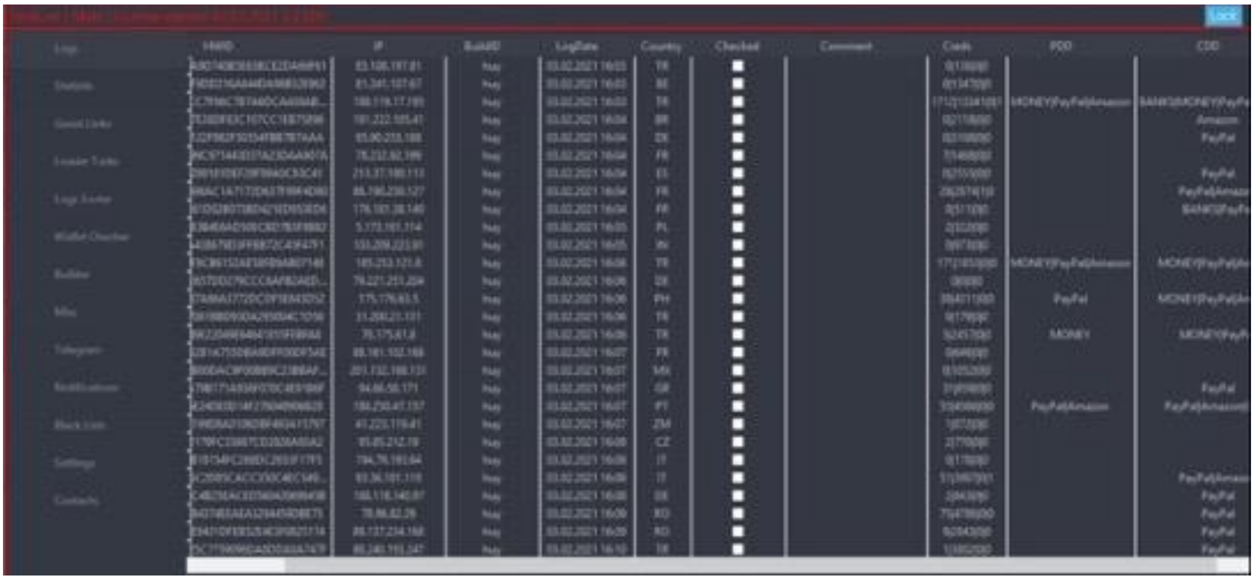
1. **Logs selling**

One of the most common types of cybercrimes is the log selling. Cybercriminals got access to the logs in different ways. The most often stolen logs can provide access to the bank accounts by using email logins and other credentials (like Booking, Netflix, Steam etc.). Another prominent cybercrime niche is the social media breaking. The most popular techniques which are used to get access to the logs are phishing, social engineering, brute force and checkers and stealers.

- **Phishing** is a type of cybercrime that targets victims by sending them a fake link to the webpage which appears as a well-known source where the victim put their personal data which is subsequently transferred to the cybercriminal.
- **Social Engineering** is a type of cybercrime that uses psychological manipulation to trick victims into making security mistakes or giving away sensitive information. One example of social engineering is romance scamming, when the cybercriminal creates a fake account on the meeting website and convinces a victim to, for example, transfer him money.
- **Stealing through brute force-accounts or checkers:** brute force is basically submitting many passwords or passphrases with the hope of eventually guessing correctly. Checker is almost the same as brute force, but checker program also can check if there is some useful information or money on the accounts. For example, the cybercriminal can attack an account of a victim on Steam and check if there are some games on this account. By doing

this the criminal can make sure that this account is valuable and thereby he or she can sell it on the underground market for a higher price.

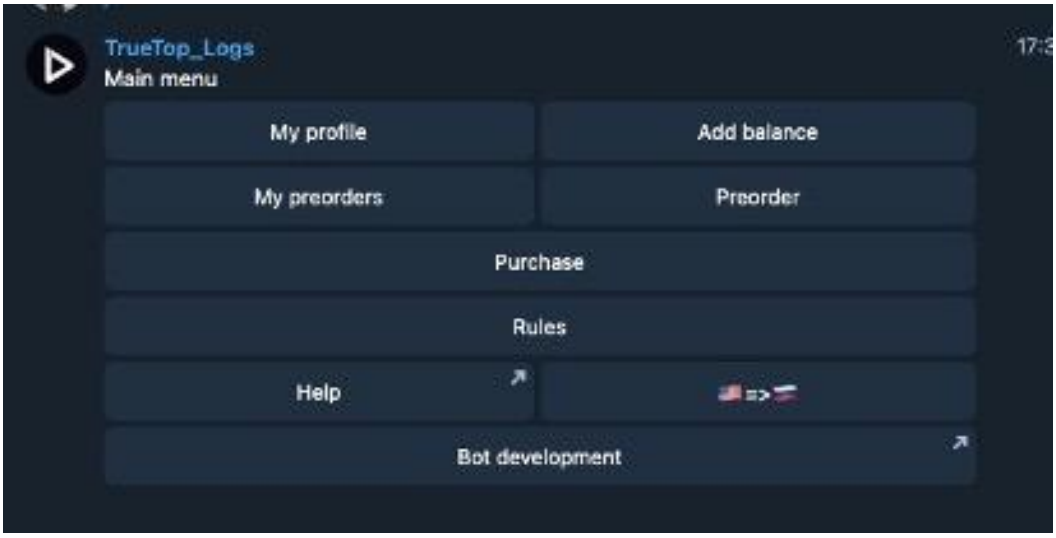
- **Stealer** is an illegal software which activates exe. files on the victim's computer and stole all the data without even knowing of the victim. One of the most relevant examples of this is a RedLine Stealer. Stealer is the most advanced type of the log stealing attack, which requires strong technical training of a cybercriminal. The price for the RedLine stealer on the underground market starts from the 200$, but in most of the cases it also requires a purchase of the manual to the stealer, which can go up to 500$. Usually, the launch of a stealer requires some preparation actions, for example, the use of social engineering or phishing techniques in order to receive access to some of the victim's data.



Pic. 1. Example of the RedLine interface[5].

When cybercriminals gain access to the logs, they can either sell it or use them in further illicit actions. For the cybercriminal it is not profitable to sell the logs one by one, because some of the gained logs can be already "compromised" by the owner (e.g., when the owner realized when his or her data was stolen and changed the password), and thereby they often choose the way through sell the pack of logs through the bots on the Telegram. A price for the pack of logs (100-200 logs in a pack) starts from approximately 1$ for one log.

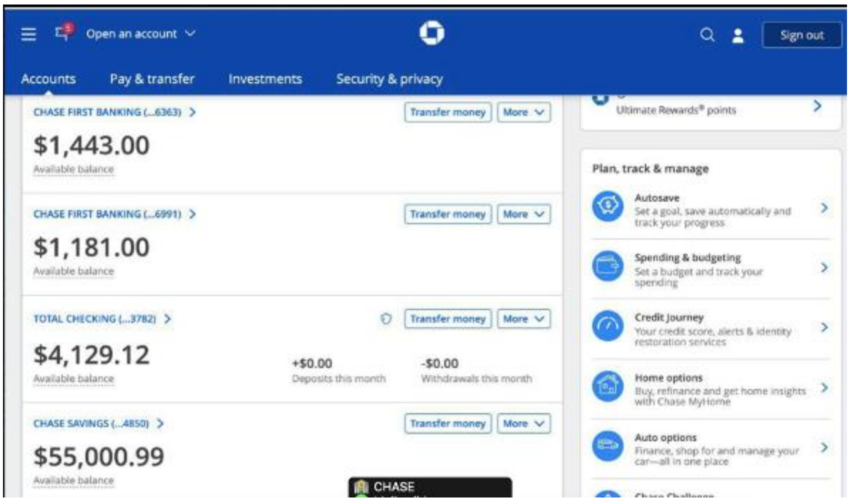
[5] Evidence-Based Cybersecurity Research Group. Retrieved from https://ebcs.gsu.edu.



Pic. 2. Example of the log selling bot in Telegram[6].

The price for the selling logs relies deeply on the quality of the stolen logs. The most precious ones are the logs which are called the “full-info”. Basically, this is the log which contains the fullest information on the victim - for example: name, surname, address, Social Security Number (SSN). An example of the imaginary full info is the following one:

DIEDRA | A HICKEY | 1055 TRENTON CT | ATLANTIC BEACH | FL | 32233 |
diedramurphy@hotmail.com || 9042468720 | 241333860 | 1978-04-12 | 1978 |



CHASE FIRST BANKING (...6363)
$1,443.00
Available balance

CHASE FIRST BANKING (...6991)
$1,181.00
Available balance

TOTAL CHECKING (...3782)
$4,129.12
Available balance
+$0.00
Deposits this month
-$0.00
Withdrawals this month

CHASE SAVINGS (...4850)
$55,000.99
Available balance

CHASE

Ultimate Rewards® points

Plan, track & manage

Autosave
Set a goal, save automatically and track your progress

Spending & budgeting
Set a budget and track your spending

Credit Journey
Your credit score, alerts & identity restoration services

Home options
Buy, refinance and get home insights with Chase MyHome

Auto options
Finance, shop for and manage your car—all in one place

Chase Challenge

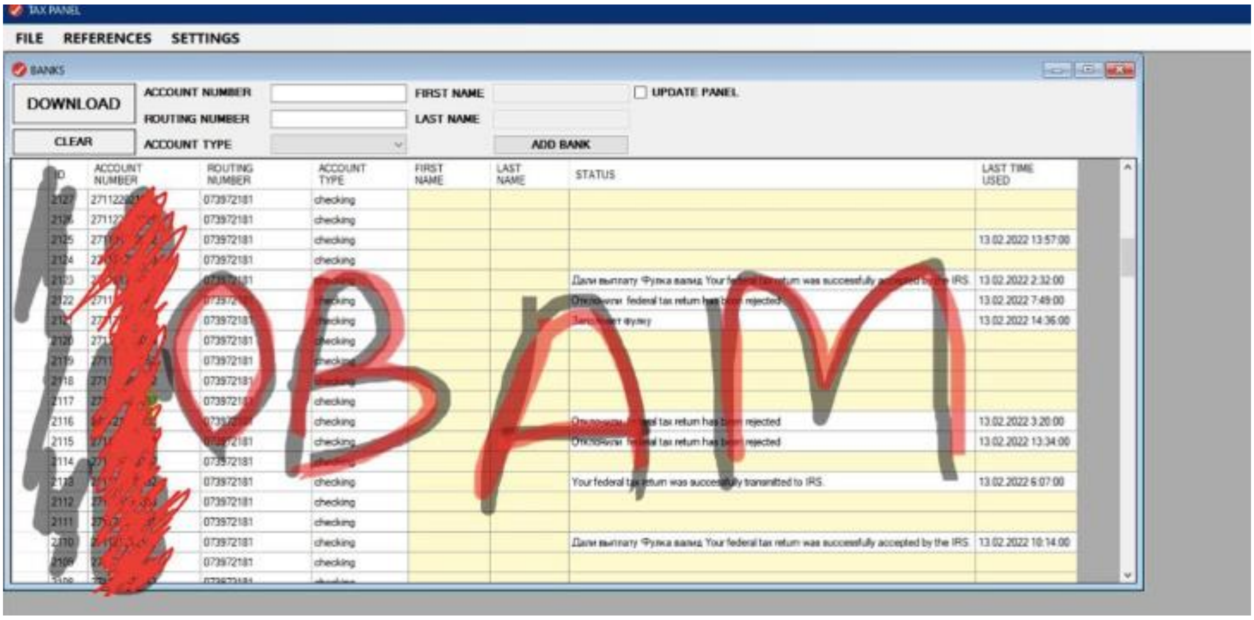
Pic. 3. A stolen log can help cybercriminals to get access to the victim’s bank account[7].

[6] Evidence-Based Cybersecurity Research Group. Retrieved from https://ebcs.gsu.edu.
[7] *Ibid.*

2. Steal of Social Payments

Social payments are a part of the social programs aimed to support the population in the United States. It includes many types of financial support, which became especially relevant during the Covid-19 pandemic. The most common are the Pandemic Unemployment Assistance (PUA), loans from Small Business Administration (SBA) and also the tax returns from the Internal Revenue Service (IRS).

Unfortunately, these kinds of social payments are most susceptible to theft. When the cybercriminal receives full info, he can check whether the victim is eligible to receive the social payment. This is applicable both to individuals and to the companies, especially the small business. Another point of interest for the cybercriminals are the immigrants, particularly the individuals who come to the United States on the Work & Travel type of visa. These people usually do not even know that they are eligible to receive a tax return that cybercriminals actively use. For example, in the case of the tax return, the cybercriminal uses his own database or the purchased full info and with a help of the software (e.g., the TurboTax, which is generally a legit software for filing taxes online) just try to fill in the tax return forms with this data in order to receive the money.

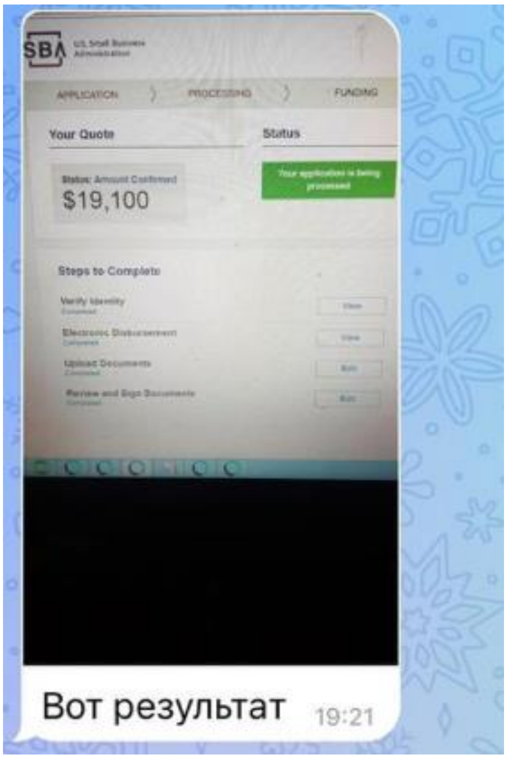


ID	ACCOUNT NUMBER	ROUTING NUMBER	ACCOUNT TYPE	FIRST NAME	LAST NAME	STATUS	LAST TIME USED
[redacted]	[redacted]	073972181	checking				
[redacted]	[redacted]	073972181	checking				
[redacted]	[redacted]	073972181	checking				13.02.2022 13:57:00
[redacted]	[redacted]	073972181	checking				
[redacted]	[redacted]	073972181	checking			Дали выплату Фулка валид Your federal tax return was successfully accepted by the IRS	13.02.2022 2:32:00
[redacted]	[redacted]	073972181	checking			Отклонили federal tax return has been rejected	13.02.2022 7:49:00
[redacted]	[redacted]	073972181	checking			Заполняет фулку	13.02.2022 14:36:00
[redacted]	[redacted]	073972181	checking				
[redacted]	[redacted]	073972181	checking				
[redacted]	[redacted]	073972181	checking				
[redacted]	[redacted]	073972181	checking				
[redacted]	[redacted]	073972181	checking			Отклонили federal tax return has been rejected	13.02.2022 3:20:00
[redacted]	[redacted]	073972181	checking			Отклонили federal tax return has been rejected	13.02.2022 13:34:00
[redacted]	[redacted]	073972181	checking				
[redacted]	[redacted]	073972181	checking			Your federal tax return was successfully transmitted to IRS.	13.02.2022 6:07:00
[redacted]	[redacted]	073972181	checking				
[redacted]	[redacted]	073972181	checking				
[redacted]	[redacted]	073972181	checking			Дали выплату Фулка валид Your federal tax return was successfully accepted by the IRS.	13.02.2022 10:14:00
[redacted]	[redacted]	073972181	checking				

Pic. 3. A screenshot posted by the cybercriminal in the Telegram channel from TurboTax[8].

Companies' social payments also became a target for the cybercriminals, who actively use the SBA loans and other Covid-19 help for the eligible businesses.

[8] Evidence-Based Cybersecurity Research Group. Retrieved from https://ebcs.gsu.edu.



SBA U.S. Small Business Administration

APPLICATION 〉 PROCESSING 〉 FUNDING

Your Quote

Status: Amount Confirmed

$19,100

Status

Your application is being processed

Steps to Complete

Verify Identity
Completed

Electronic Disbursement
Completed

Upload Documents
Completed

Review and Sign Documents
Completed

Вот результат 19:21

Pic. 4. A review from a Telegram channel from the person who sold the full info for illicit activities. Cybercriminal just received $19,100 from the SBA loan[9].

3. Money Laundering

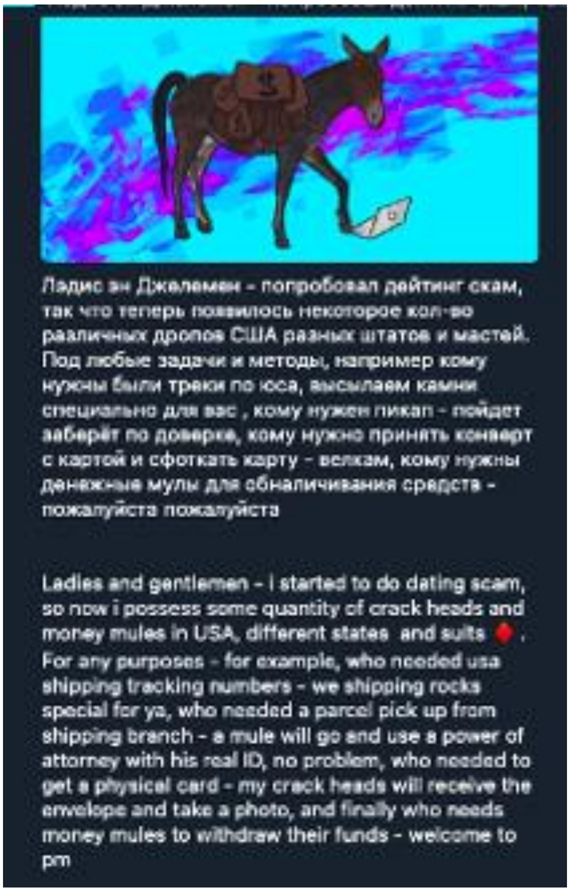
Once the cybercriminal gets access to the bank account or finds out that the victim is eligible for the social payment, he or she needs to withdraw the money the way it cannot be traced. Like in the "traditional" crime, the cybercriminals use a process which is called "money laundering" or "cash-out". By doing this, cybercriminals will be able to make large amounts of money received from the cybercrime appear to have come from a legitimate source. There are multiple ways of money laundering but the most popular are made through self-registered accounts or through the group of people called "mules".

Self-registered accounts are the accounts in popular money-transfer services and wallets like PayPal and MoneyLion or bank accounts, which are registered on the fictitious or stolen data without mentioning the cybercriminal's credentials. Cybercriminals can even use the stolen biometric data or scans of identifying documents of the victim to pass the authentication in these services or use the documents rendering in order to create a fake account. Then cybercriminals can transfer the compromised money from the target or the stolen social payments and using the self-registered account make this transfer look completely legit. Usually, cybercriminals use the

[9] Evidence-Based Cybersecurity Research Group. Retrieved from https://ebcs.gsu.edu.

services of the criminal group called “call-centers”, where trained people call by the request to banks and other services and help cybercriminals to confirm their fake “personality”.

Another way to launder money is using the “mules”. “Mules” are divided into two groups: the first one does the laundering by their own will, in most cases for the remuneration, another one are made to do the laundering, being the victim of the social engineering (e.g. many cybercriminals use the romance scams also in order to find the mules).



Ладис эн Джелемен - попробовал дейтинг скам, так что теперь появилось некоторое кол-во различных дропов США разных штатов и мастей. Под любые задачи и методы, например кому нужны были треки по юса, высылаем камни специально для вас , кому нужен пикап - пойдет заберёт по доверке, кому нужно принять конверт с картой и сфоткать карту - велкам, кому нужны денежные мулы для обналичивания средств - пожалуйста пожалуйста

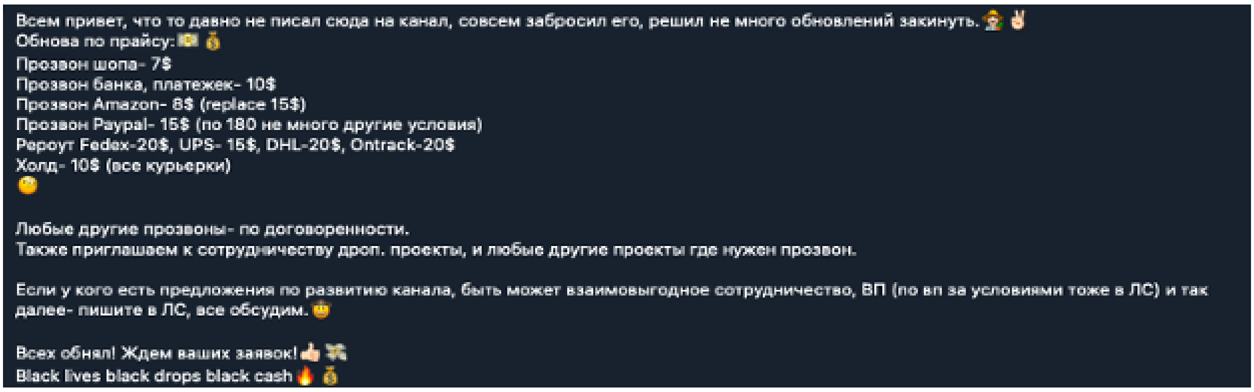
Ladies and gentlemen - i started to do dating scam, so now i possess some quantity of crack heads and money mules in USA, different states and suits ♦ . For any purposes - for example, who needed usa shipping tracking numbers - we shipping rocks special for ya, who needed a parcel pick up from shipping branch - a mule will go and use a power of attorney with his real ID, no problem, who needed to get a physical card - my crack heads will receive the envelope and take a photo, and finally who needs money mules to withdraw their funds - welcome to pm

Pic. 5. Cybercriminal put an advertisement on providing the “mules” services from romance scams[10].

4. Carding

Carding is a common name for all the cybercrimes which jeopardize the credit cards and checks, including the laundering and stolen logs from the bank accounts. Due to its prevalence and danger, carding took a special place among all cybercrimes. Usually carding is linked with cash-out of the compromised cards and buying goods, prepaid gift-cards and gift-certificates and then reselling it on the underground markets. Carding is closely linked with “call-center” activity.

[10] Evidence-Based Cybersecurity Research Group. Retrieved from https://ebcs.gsu.edu.



Всем привет, что то давно не писал сюда на канал, совсем забросил его, решил не много обновлений закинуть. 👨‍🌾 ✌️
Обнова по прайсу: 💴 💰
Прозвон шопа- 7$
Прозвон банка, платежек- 10$
Прозвон Amazon- 8$ (replace 15$)
Прозвон Paypal- 15$ (по 180 не много другие условия)
Pepoyт Fedex-20$, UPS- 15$, DHL-20$, Ontrack-20$
Холд- 10$ (все курьерки)
😳

Любые другие прозвоны- по договоренности.
Также приглашаем к сотрудничеству дроп. проекты, и любые другие проекты где нужен прозвон.

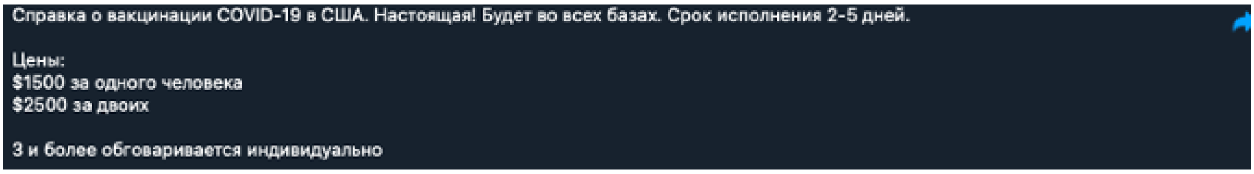
Если у кого есть предложения по развитию канала, быть может взаимовыгодное сотрудничество, ВП (по вп за условиями тоже в ЛС) и так далее- пишите в ЛС, все обсудим. 🤠

Всех обнял! Ждем ваших заявок! 👍 💸
Black lives black drops black cash 🔥 💰

Pic. 6. This "call-center" can make calls for Amazon, Bank, PayPal, delivery services, etc. Basically, if a cybercriminal has full info about the victim and their card credentials, they can ask the "call-center" to cash them out. For example, they see that the victim has the pending order from Dyson on some expensive vacuum cleaner. Then the cybercriminal asks the "call-center" to call Dyson in order to make a "reroute" - this is the name of the service when the "call-center" changes the delivery point from the victim to cybercriminal. In order to sound legit, the "call-center" can just "confirm" the credentials with the full info (and credit card number[11]).

5. Fake Documents

The Dark Web became one of the most popular markets for selling the fake documents. The types of the fake documents range dramatically starting from the fake driver licenses and passports and ending with the fake Covid-19 vaccination cards. Definitely, the quality of the fake documents deeply depends on the price: for example, for $1500 the buyer will receive not only the fake Covid-19 vaccination card which looks indistinguishable from the real one, but also his or her data will be inserted in the base of the people who really received a vaccination.



Справка о вакцинации COVID-19 в США. Настоящая! Будет во всех базах. Срок исполнения 2-5 дней.

Цены:
$1500 за одного человека
$2500 за двоих

3 и более обговаривается индивидуально

Pic. 7. Fake Covid-19 Vaccination cards which are available to use in the USA (the price is $1500)[12].

3. Techniques and Methods of the Cybercrime Investigation

After identification of the type of the cybercrime, the law enforcement bodies are starting to use the various techniques to provide the investigation. Although the types of the "traditional" crimes and the cybercrimes are similar, due to the peculiarities of the cybercrime, including the cross-border character, techniques which are suitable for the "traditional" crime investigation usually cannot be applicable to the cybercrimes.

[11] Evidence-Based Cybersecurity Research Group. Retrieved from https://ebcs.gsu.edu.
[12] *Ibid.*

Thus, differences between the cybercrime and "traditional" crime investigation can be presented the following way:

	"Traditional" Crime Investigation	**Cybercrime Investigation**
Steps	1. Initial information gathering: • Searching and interviewing of witnesses and victims • Conducting a search for evidence and gathering physical evidences • Reconstruction of a Crime Scene 1. Reporting of the results of investigation 2. Prosecution 3. Trial	1. Initial information gathering: • Searching and interviewing of victims • Conducting a search for electronic evidences • Reconstruction of a Digital Crime Scene 1. Reporting of the results of investigation 2. Prosecution 3. Trial
Evidences	1. Physical Evidence (e.g. fingerprints, DNA samples, murder weapons etc.) 2. Demonstrative Evidence (e.g. photo- and video-evidences) 3. Documentary Evidence (evidence in the form of documents) 4. Witness Testimony	1. Electronic Evidence (e.g. electronic conversations, source/object code etc.) 2. Material Evidences (e.g. USB-cards, computers etc.)
Actors	Criminal Justice Agencies (Law Enforcement Bodies, Forensic Scientist (on the request) Prosecutors, Judges)	Criminal Justice Agencies (Law Enforcement Bodies, Digital Forensics, Prosecutors, Judges), National Security Agencies, Private companies
Required Skills	1. Criminological Skills (knowledge on work with judicial process, including the presentation of facts and evidence) 2. Legal Skills (knowledge of applicable statutes, laws, regulations on conducting of the crime investigation)	1. Criminological Skills (knowledge on work with judicial process, including the presentation of facts and evidence) 2. Legal Skills (knowledge of applicable statutes, laws, regulations, and policies governing cyber targeting and exploitation, knowledge of electronic evidence law) 3. Technical Skills (Knowledge of cybersecurity and privacy principles, knowledge of electronic devices).

Table 1. Steps of the "Traditional" Crime and Cybercrime Investigation

As the one can see from the Table 1, the first step of the cybercrime investigation - initial information gathering - is a similar to the "traditional" crime, but due to the peculiarities linked to the place of commitment of the cybercrime, which is in the most of the cases happened through the ICTs, the Internet and the electronic devices, the methods used by the law enforcement agencies are rather differ from the methods used in the "traditional" crime investigations.

3.1. Digital Forensics

Basically, the evidence used in the cybercrime investigation can be collected under the practices of digital forensics. According to Ferrazzano, the aim of digital forensics is to "apply scientific and analytic techniques to digital data stored on digital devices or moving across a digital network, so as to identify, process, and preserve such data, in such a way that it can be assessed as evidence at trial"[13].

Understanding of digital forensics requires analysis of both the technical and organizational means. According to ENISA, digital forensics is divided into five main fields by the criterion of the device or technology used for the conduction of the digital forensics: network forensics, host (computer) forensics, mobile forensics, memory cloud forensics and cloud forensics[14].

3.1.1. Network Forensics

Network forensics is the practice of the monitoring and analysis of computer network traffic for the purposes of information gathering, legal evidence, or intrusion detection[15]. Usually, the information here is obtained through the network logs or the network traffic captures. The network logs are files that contain a record of events that occurred in the layers of the network. The investigation of the logs of the networks is available to the security operation officers and others non-government cybercrime investigators, as logs do not contain personal data *per se*. However, logs do contain IP-addresses, which is considered as personal data, because they can be used for the identification of the user (see, in this regard, Part 4).

Network traffic, on its turn, is all the data which moves across a network. Because it contains personal data and even sensitive information, the capture of the network is available only to the law enforcement bodies which have the legal authority to undertake this type of monitoring and interception of data[16].

[13] Caianiello, M., Camon, A. (Eds.). (2021), *Digital forensic evidence. Towards common European standards in antifraud administrative and criminal investigations, Wolters Kluwer.* p. 14.

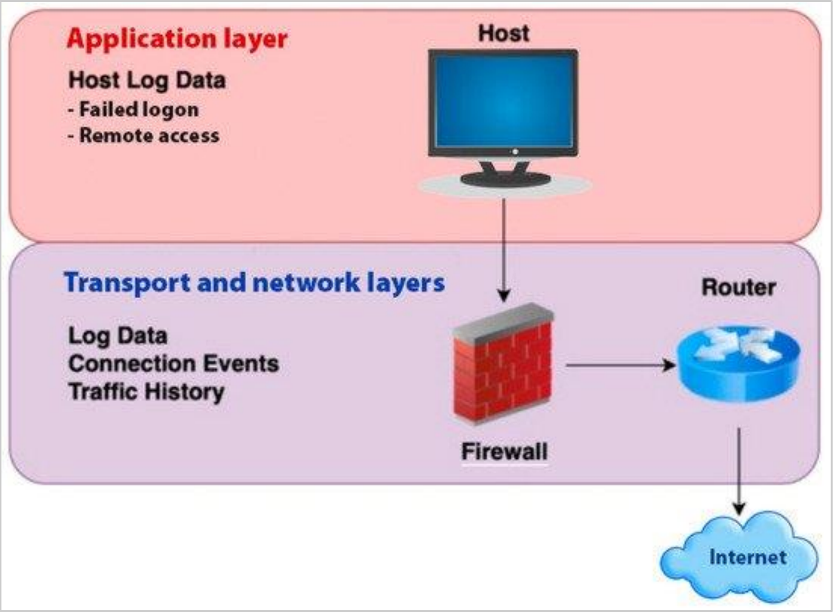
[14] ENISA. (2019). *Introduction to Network Forensics*, p. 10.

[15] *Ibid.*

[16] Kisswani, N. M. (2011). *Telecommunications (interception and access) and its regulation in Arab countries. International Journal of Liability and Scientific Enquiry, 4(1), 44*, p. 47.

Of course, one of the most popular networks where cybercrime could happen is the Internet. TCP/IP Model consists of the four layers: application layer, transport layer, interface layer and the network layer. Network forensics investigate only the application, transport, and the network layers because the network interface layer is responsible for the physical connection to the network which is not relevant for the types of the cybercrimes described in the previous parts[17]. Application layer contains information regarding failed or successful logins and the transport and network layer contain the instrument for the traffic filtering which is called the firewall. A firewall is a network security device that monitors traffic to or from the network. The data from these layers can give investigators information about potentially malicious traffic[18].

The network forensics also can help to discover the location and identification of a cybercriminal using the network information, which is gathered by the Internet Service Providers (ISPs). The possibility of getting information from the ISPs depends on the type of service, and the logging policy.



Pic. 8. This scheme shows the relationship between the layers and the information that cybercrime investigators can gather by analyzing the logs through the network forensics[19].

[17] ENISA. (2019). Introduction to Network Forensics, p. 10.

[18] Horan, C., Saiedian, H. (2021). *Cyber Crime Investigation: Landscape, Challenges, and Future Research Directions, Journal of Cybersecurity and Privacy 1, no. 4.* p. 580-596.

[19] Kisswani, N. M. (2011). Telecommunications (interception and access) and its regulation in Arab countries. International Journal of Liability and Scientific Enquiry, 4(1), 44, p. 47.

3.1.2. Host (Computer) Forensics

Host forensics is the most basic type of the digital forensics, and it is linked with an analysis of the data from the computer and other physical ICTs devices (personal computers (PCs), servers, hardware devices, etc.). The object of interest here for the digital forensic examiner is the data contained in the hard drive or computer memory.

The host forensics tools can be considered a little outdated but ENISA highlights that in order to provide a full cybercrime investigation it is necessary to analyze the information gathered from both the methods[20]. Thus, the network forensics cannot tell what happened with the packet data before it enters the network, for example, which processes sent and/or received the packets, what they did with it, etc.

3.1.3. Mobile Forensics

Mobile device forensics helps to recover electronic evidence from mobile devices[21]. Under the term "mobile device" typically is understood mobile phones, but in reality, the mobile device forensics examiners can also investigate all the devices that are mobile (can be carried around) and have an opportunity to provide wireless network connection, for example, tablets, laptops, wearables, etc.[22].

It is one of the most sensitive parts of digital forensics because mobile devices usually contain multiple personal data. That is why the investigation of the cybercrime should be provided carefully following the special phases of the mobile device forensics.

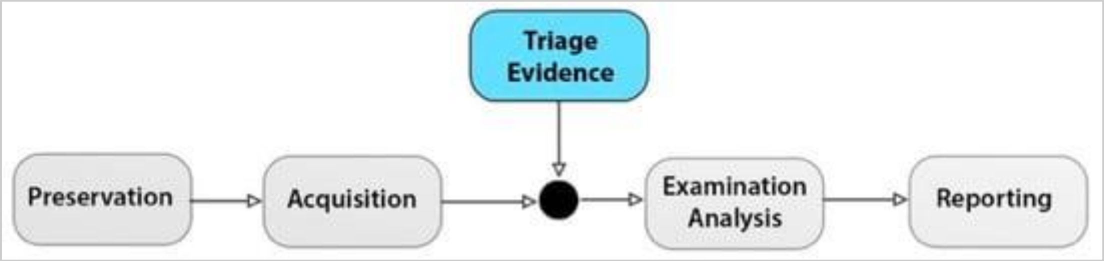
The process of the mobile device forensics consists of the four investigation steps: "preservation, acquisition, examination/analysis and reporting of digital evidence"[23]:

[20] ENISA. (2019). Introduction to Network Forensics, p. 10.

[21] NIST. (2019). *Guidelines on Mobile Device Forensics,* p. 27.

[22] ENISA. (2019). Introduction to Network Forensics, p. 12.

[23] Barmpatsalou, K., Cruz, T., Monteiro, E., & Simoes, P. (2018). *Current and Future Trends in Mobile Device Forensics. ACM Computing Surveys, 51(3), p. 5.*



Pic. 9. Mobile device forensics steps[24].

The investigation starts from the *preservation* phase, where the mobile devices are taken by the investigators and tracking their state in order to ensure that the content will stay there during all the investigation. Then, at the *acquisition* phase, the mobile forensics examiner is extracting the data by copying it to another device to provide further *examination*. During this phase the extracted data is made clean, also from the personal data details, and is analyzed to provide a final report through the reporting stage.

3.1.4. Memory Forensics

Memory Forensics is the process of investigating the storage in the device, the subject matter of which is the identifying of the traces of the cybercrime in the device's memory. Device's memory, for example, computer memory is usually divided into two parts: Primary Memory (RAM and ROM) and Secondary Memory (hard-drives, USB, CD etc.). RAM stands for "Random Access Memory," and is the volatile memory and ROM is "Read-Only Memory", which is a non-volatile memory. Data which is placed in the non-volatile memory cannot be erased when the power of the device is removed. ENISA highlights that memory forensics "is the only method of investigation that remains usable, when the cybercriminals do not write data to the system's non-volatile storage (ROM) during a cybercrime attack".

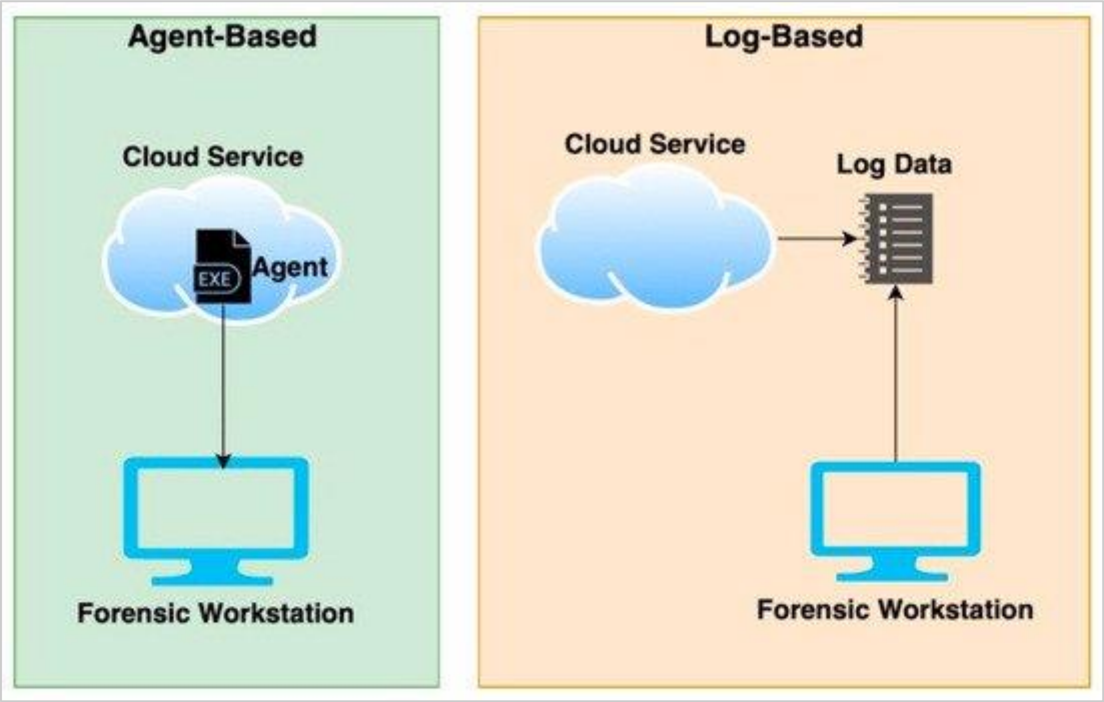
Besides the memory forensics examiner can also investigate the other Primary Memory information, like the RAM data, which in contrast will be deleted immediately after the system reboot or the power is off, i.e., the processes in the kernel (the operating system). The Secondary memory is usually investigated by the host (computer) forensics examiner.

3.1.5. Cloud Forensics

[24] *Barmpatsalou, K., Cruz, T., Monteiro, E., & Simoes, P. (2018). Current and Future Trends in Mobile Device Forensics. ACM Computing Surveys, 51(3), p. 5.*

Cloud forensics is focused on the investigation of cybercrimes which involve cloud technologies. This type of digital forensics can help to investigate data breaches and identity thefts. Manral proposed to divide cloud forensics into two sections: agent-based solutions and log-based solutions[25]. Log-based solutions consist in the direct examination of the logs on the cybercrime incident, storing in the cloud, and based on the type of the logs are divided into four kinds of cybercrime investigations: incident-driven, provider-driven, consumer-driven, and resource-driven investigations[26].

Agent-based solutions rely on the application or the agent which collects the information regarding the cybercrime incident and sends it back in order to be analyzed by the cloud forensics examiner.



Pic. 10. Difference between the agent-based and log-based cloud forensics[27]

3.2. Intelligence Activities

[25] Manral, B., Somani, G., Choo, K.-K. R., Conti, M., & Gaur, M. S. (2019). *A Systematic Survey on Cloud Forensics Challenges, Solutions, and Future Directions. ACM Computing Surveys, 52(6),* p. 7.

[26] NIST. (2019). Guidelines on Mobile Device Forensics, p. 4.

[27] Manral, B., Somani, G., Choo, K.-K. R., Conti, M., & Gaur, M. S. (2019). A Systematic Survey on Cloud Forensics Challenges, Solutions, and Future Directions. ACM Computing Surveys, 52(6), p. 7.

Intelligence activities in the cybercrime investigation sphere include mainly the activities on the Internet. The main type of collecting the information on the Internet is Open-source intelligence (OSINT) methods. Besides that, undercover operations, decoys, and other “traditional” intelligence activities are also conducted on the Internet and according to Jang are even easier because of the anonymity which is provided by the online activities[28]. The OSINT can be used by any cybercrime investigators, including the usual users. As Giacomello and Eriksson fairly mentioned, the interesting thing about the OSINT activities is that they basically are the antithesis of the cybercrime, as the techniques used for the cybercrime investigation can be used as a cyberattack, and vice versa[29].

As was mentioned in the previous Part, the main fields for the intelligence activities are the Surface Web, the Deep Web, and the Dark Web. The Surface Web can provide a lot of useful information for the investigators, and it can be mined easily in order to construct the full picture of the cybercrime investigation. The Deep Web information can help to identify cybercriminals using the information gathered from the Surface Web, for example, their social media accounts.

The Dark Web is the main source of the information for the cybercrime investigation as it contains “live” activities of the cybercriminals through the Dark Web forums. Nazah proposes to divide the cybercrimes which can be investigated through the Dark Web sources into eight main groups: human trafficking and sex trafficking, pornography industry, assassinations and its marketing, drug transactions, child pornography, terrorism, markets for cybercrime tools and stolen data and the Dark Net currency exchange using bitcoin[30]. Thus, the highlighted categories are almost identical to the ones proposed by the author in the previous Part.

3.3. Honeypots

A honeypot is an instrument of the attraction of the cybercriminal to the aim (usually, the virtual machine (VM) specifically created for this reason), with an intention to open the security vulnerabilities and evidence of the cyberattack. Thus, a honeypot (or a honeynet) is intentionally made to be compromised in order to gather and analyze the information about the methods and procedures which the cybercriminal uses. The honeypot which is used incorrectly can lead to the legal challenges of the cybercrime investigation, discussed in the following parts.

[28] Jang, Y. (2009). *Best Practices in Cybercrime Investigation in the Republic Korea, UNAFEI, Resource Material Series No. 79,* p. 59.

[29] Eriksson, J., & Giacomello, G. (2014). *International Relations, Cybersecurity, and Content Analysis: A Constructivist Approach. The Global Politics of Science and Technology - Vol. 2,* p.144.

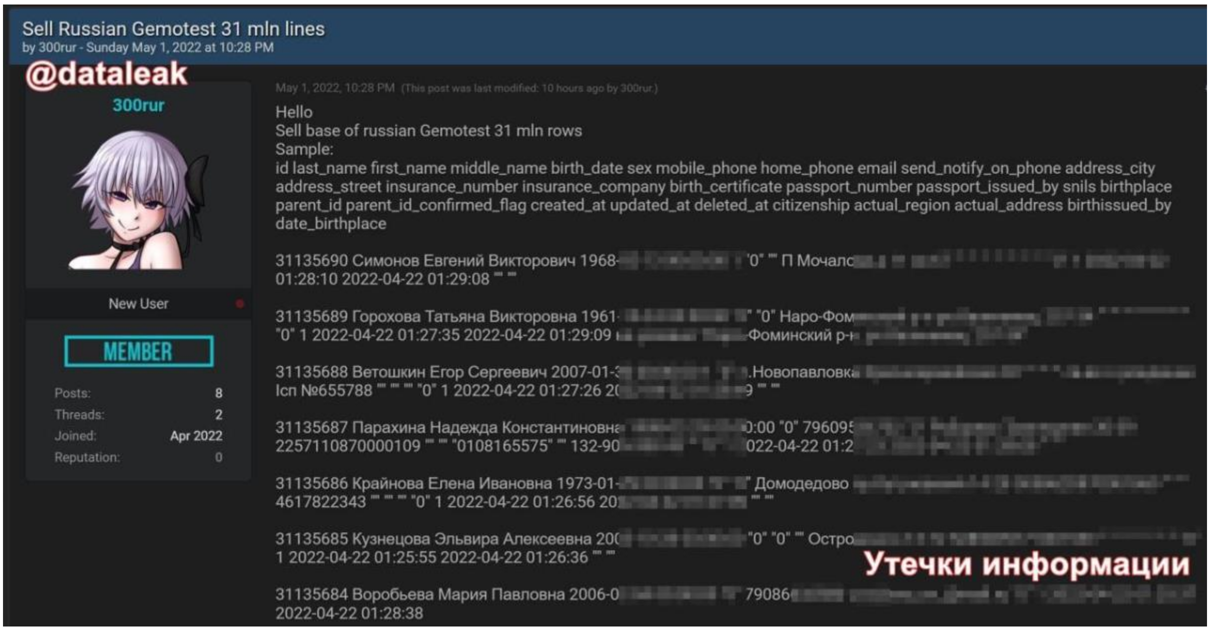
[30] Nazah, S., Huda, S., Abawajy, J. H., & Hassan, M. M. (2020). *Evolution of Dark Web Threat Analysis and Detection: A Systematic Approach. IEEE Access,* p. 5.

4. Cybercrimes That Compromise Personal Data

Cybercrimes compromising personal data are among the most spreading crimes in the sphere of informational technologies. These types of crimes violate both the security and privacy of the data, as data is considered as a commodity not only for the legal purposes but also for the cybercriminals.

The main reason for the data to become an object of the cybercrime is a data breach. Data breaches usually happen due to human factors, for example, from the stolen or lost devices, or technical factors, like poor security, the unauthorized access to the database (hacking) or accidental disclosure of data to the public.

One of the biggest data breaches happened in 2013, when more than three billion Yahoo users' data was leaked, including the victims' names, email addresses and passwords. According to the "Cost of Data Breach Report", the average damage of a data breach in 2021 was $4,24 million with an increase of more than 10% from 2020[31]. Interestingly enough, the economic sector with the highest number of breaches is healthcare ($9,23 million in 2021)[32] and the United States became the country with the highest number of damages in the world ($9,05 million in 2021)[33], both for 11 years in a row. Thus, in May 2022, a database containing personal data of more than 30 million clients from the Russian medical laboratory Gemotest was leaked to one of the Darknet forums (pic. 11).



Sell Russian Gemotest 31 mln lines
by 300rur - Sunday May 1, 2022 at 10:28 PM

300rur

New User

MEMBER

Posts: 8
Threads: 2
Joined: Apr 2022
Reputation: 0

May 1, 2022, 10:28 PM (This post was last modified: 10 hours ago by 300rur.)

Hello
Sell base of russian Gemotest 31 mln rows
Sample:
id last_name first_name middle_name birth_date sex mobile_phone home_phone email send_notify_on_phone address_city address_street insurance_number insurance_company birth_certificate passport_number passport_issued_by snils birthplace parent_id parent_id_confirmed_flag created_at updated_at deleted_at citizenship actual_region actual_address birthissued_by date_birthplace

```
31135690 Симонов Евгений Викторович 1968-[redacted] '0" "" П Мочалс[redacted]
01:28:10 2022-04-22 01:29:08 "" ""

31135689 Горохова Татьяна Викторовна 1961-[redacted]" "0" Наро-Фом[redacted]
"0" 1 2022-04-22 01:27:35 2022-04-22 01:29:09 [redacted]Фоминский р-[redacted]

31135688 Ветошкин Егор Сергеевич 2007-01-[redacted].Новопавловк[redacted]
Iсп №655788 "" "" "" "0" 1 2022-04-22 01:27:26 2[redacted]9 "" ""

31135687 Парахина Надежда Константиновна[redacted]0:00 "0" 79609[redacted]
2257110870000109 "" "" "0108165575" "" 132-90[redacted]022-04-22 01:2[redacted]

31135686 Крайнова Елена Ивановна 1973-01-[redacted]" Домодедово [redacted]
4617822343 "" "" "" "0" 1 2022-04-22 01:26:56 20[redacted] "" ""

31135685 Кузнецова Эльвира Алексеевна 20[redacted]"0" "0" "" Остро[redacted]
1 2022-04-22 01:25:55 2022-04-22 01:26:36 "" ""

31135684 Воробьева Мария Павловна 2006-0[redacted] 79086[redacted]
2022-04-22 01:28:38
```

Pic. 11. The advertising posted on the Darknet Forum with the leaked database from Russian medical laboratory Gemotest[34]

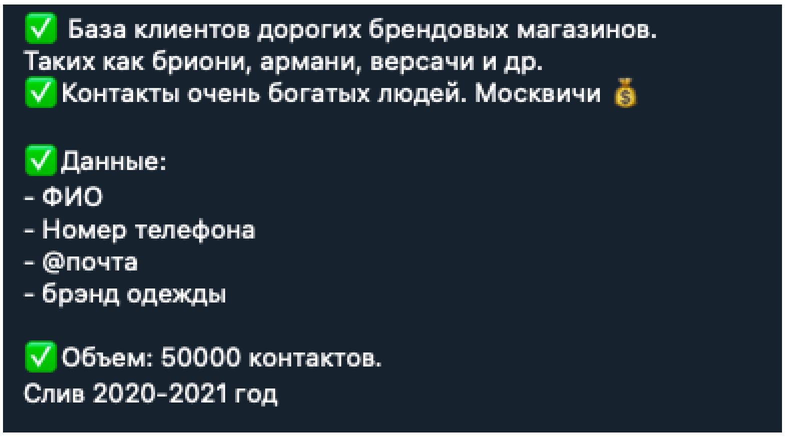
[31] IBM. (2021). *Cost Of a Data Breach Report*, p. 4.

[32] *Ibid.*, p. 14.

[33] *Supra* note 31.

[34] Evidence-Based Cybersecurity Research Group. Retrieved from https://ebcs.gsu.edu.

Most of the stolen data is published in the Dark Web forums and the Telegram channels, usually for a reward. The price for the leaked data differs due to the amount of the data and the quality. For example, according to the Dark Web Price Index 2022, published by the Privacy Affairs, one stolen scan of Russian passport costs 100$ and the leaked logins from the social media and email start from 45$ for a piece (pic. 13)[35].

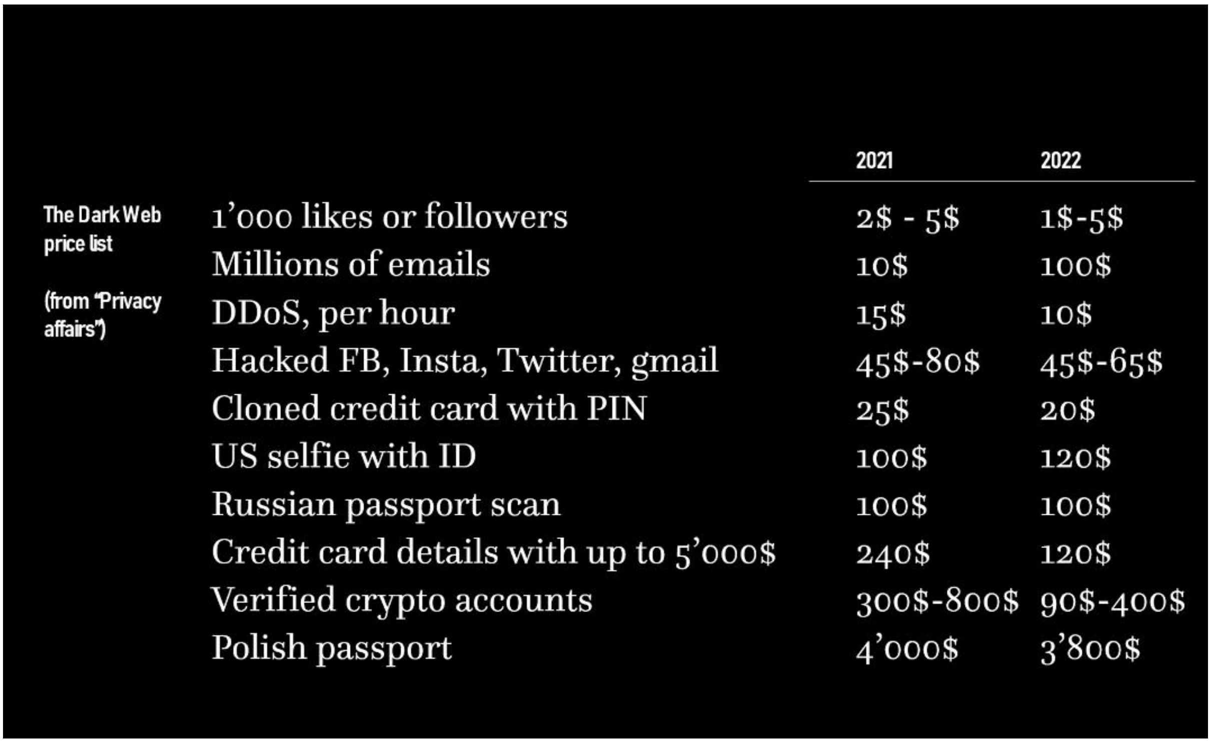


✅ База клиентов дорогих брендовых магазинов. Таких как бриони, армани, версачи и др.
✅ Контакты очень богатых людей. Москвичи 💰

✅ Данные:
- ФИО
- Номер телефона
- @почта
- брэнд одежды

✅ Объем: 50000 контактов.
Слив 2020-2021 год

Pic. 12. The stolen database with name, surname, mobile phone and email of the customers from luxury stores in Moscow. This database includes data for 50000 customers[36].



The Dark Web price list

(from "Privacy affairs")

	2021	2022
1'000 likes or followers	2$ - 5$	1-5
Millions of emails	10$	100$
DDoS, per hour	15$	10$
Hacked FB, Insta, Twitter, gmail	45-80	45-65
Cloned credit card with PIN	25$	20$
US selfie with ID	100$	120$
Russian passport scan	100$	100$
Credit card details with up to 5'000$	240$	120$
Verified crypto accounts	300-800	90-400
Polish passport	4'000$	3'800$

Pic. 13. The Dark Web Price List 2022 (slide from the presentation of Andrzej Nowak).

[35] Dark Web Price Index 2022 - Dark Web Prices of Personal Data. Privacy Affairs. (2022, March 16). Retrieved May 12, 2022, from https://www.privacyaffairs.com/dark-web-price-index-2022/.
[36] Evidence-Based Cybersecurity Research Group. Retrieved from https://ebcs.gsu.edu.

In addition, leaked data is used for blackmailing of victims with the aim to receive a reward for not publishing the compromising information consisting of the stolen databases. For example, in 2015 hackers received an access to the base of personal information of the users of the website Ashley Madison, which helped people to find extramarital affairs[37]. Another example was the leak of the base of the customers of fake COVID-19 vaccination certificates in Russia, which contained personal information on hundreds of thousands of people. The compromised data was posted in November 2021 in Telegram channels, where 1,000 lines of the data cost $120. It contained all the information about the people who bought the fake COVID-19 certificates, including passport details, phone numbers, addresses and fake vaccination dates[38].

5. Challenges of Cybercrime Investigation

Law enforcement agencies all over the world declare many problems that they have to face in the fight against computer criminals. Due to the complex nature of cybercrime, criminal investigation of the offenses committed in cyberspace changed drastically. The main challenge is an organization of confrontation of transnational crimes and following the evidence trails, while challenging the technical, legal, and ethical obstacles[39].

5.1. The Technical Challenges of Cybercrime Investigation

Under the technical issues are understood any issues which relate to a use of technology, technological tools or methodology, concerning the cybercrime investigation. Saiedian describes the methodological one as the most basic, as still there is no unified methodology on the implementation of the technological tools and techniques in the cybercrime investigations on the national and international level (so called, "best practices")[40].

Another technical issue is the quality and the quantity of the data collected as a result of the OSINT and the Digital Forensics Intelligence (DFINT) activities. Sometimes the collected data

[37] Zetter, K. (2015, August 18). Hackers finally post stolen Ashley Madison Data. Wired. Retrieved May 12, 2022, from https://www.wired.com/2015/08/happened-hackers-posted-stolen-ashley-madison-data/.

[38] Kommersant. (2021, November 11). *Failure of the Fake Vaccination Certificates*. Retrieved May 12, 2022, from https://www.kommersant.ru/doc/5066303.

[39] *Nazah, S., Huda, S., Abawajy, J. H., & Hassan, M. M. (2020). Evolution of Dark Web Threat Analysis and Detection: A Systematic Approach. IEEE Access*, p. 7.

[40] Horan, C., Saiedian, H. (2021). *Cyber Crime Investigation: Landscape, Challenges, and Future Research Directions, Journal of Cybersecurity and Privacy 1, no. 4.* p. 580-596.

have not been verified and will become useless for the cybercrime investigation or even turn the investigation in the wrong direction. As for the quantity of the data, the so-called Big Forensics Data (BFD), gathered with the help of DFINT, which is associated with the necessity of managing the volume, velocity, and variety of the forensics data. The amount of the BFD mined during the cybercrime investigation is enormous and due to the development of the technologies, the extracted BFD can exist in various formats, which require a certain level of technical training for the investigator.[41] It is almost impossible for the cybercrime investigation to examine all single data, for example, from the log flies during the network forensics investigation, which can lead to the loss of possibly important information[42].

The diversity of devices, hardware and software utilities and kernel operating systems also put challenges before the cybercrime investigators[43]. One of the most topical issues in the cybercrime investigation is the technologies which allows the randomization of kernel addresses and IP-addresses by the cybercriminals to anonymize their location, which makes the investigation much more difficult to provide. It is interesting enough, that often the cybercrime investigators and the digital forensics examiners use the same techniques to provide investigations with a particular amount of confidentiality. Thus, it is very important for the cybercrime investigators to be familiar with the modern technologies and understand the process of collecting digital evidence using them.

5.2. The Legal Issues of Cybercrime Investigation

One of the most challenging issues in the legal field is the collection of digital evidence. Work with the digital evidence starts with the collection, which must be established in the legal way, and presented to the court. During this time the cybercrime investigators have to maintain the integrity and availability of such data and be ready to prove it. If the investigators failed to do this, such compromised evidence would become inadmissible in court and the case will be lost.

For example, when the investigators on the territory of the EU use the honeypots technique, the information gathered from the honeypot can be considered as personal data as they processed the IP-addresses of the cybercriminals. Because of that, the cybercrime investigators are considered as the controllers of the personal data, which put on them the obligation to contain the

[41] Quick, D., & Choo, K.-K. R. (2018). *Digital forensic intelligence: Data subsets and Open Source Intelligence (DFINT+OSINT): A timely and cohesive mix. Future Generation Computer Systems, 78*, p. 566.

[42] Caviglione, L., Wendzel, S., & Mazurczyk, W. (2017). *The Future of Digital Forensics: Challenges and the Road Ahead. IEEE Security & Privacy, 15(6)*, p. 14.

[43] Jang, Y. (2009). Best Practices in Cybercrime Investigation in the Republic Korea, UNAFEI, Resource Material Series No. 79, p. 57.

data about the cybercriminals only for a certain amount of time and the disclosure of the information gathered from the honeypot in court could be considered as the personal data breach[44]. Thus, the cybercrime investigators while working with the digital evidence should strike a balance between the protection of fundamental rights and the criminal justice actions.

5.3. The Ethical Issues of Cybercrime Investigation

Ethical issues appear when there is a certain moral or ethical dilemma linked with the cybercrime investigation process. For example, there are some ethical issues linked with the criminal profiling, which is the necessary step of the criminal investigation, the "traditional" one and the investigation of the cybercrime. Under "criminal profiling" is understood a process of using "the nature of a crime to create inference about the personality of the offender"[45]. Thus, the result of the OSINT and the DFINT activities can elaborate the criminal profile of the cybercriminal, or the cybercrime group gathered from the information found about these actors.

The FBI was one of the first law enforcement agencies to embrace criminal profiling in cybercrime investigations[46]. Unfortunately, criminal profiling can become a biased tool due to the improper implementation of this instrument in the cybercrime investigation and the FBI's approach was criticized for containing the cultural and geographical assumptions, due to the link to North America[47].

6. The Future of the Cybercrime Investigation

Fortunately, development of new technologies provides opportunity not only to the spread of cybercrime but also to the investigation of cybercrime investigation. Digital forensics techniques have significantly advanced due to the use of automation technologies and big data. Basically, automation technologies help the investigator to conduct part of the investigation tasks automatically with the use of programs and without human intervention. Use of automation technologies and big data in digital forensics gave rise to the use of the machine learning techniques which in turn led to the development of artificial intelligence (AI).

For instance, cybercrime investigators can understand the sources of the illegal activities with the use of Indicators of Compromise (IOC) gathered from the public data. IOC is produced

[44] Sokol, P., Míšek, J. & Husák, M. (2017). *Honeypots and honeynets: issues of privacy. EURASIP J. on Info. Security 2017, 4.*

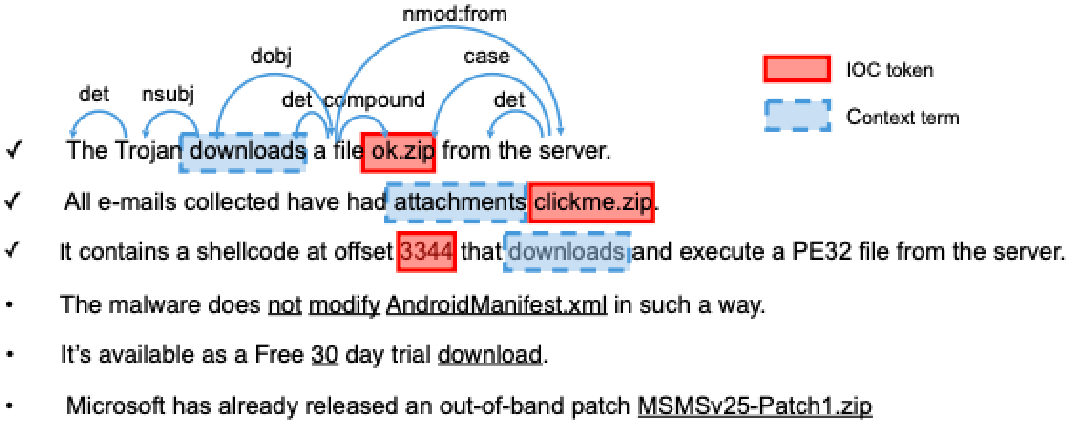
[45] Louw, D. Forensic psychology. In *International Encyclopedia of the Social & Behavioral Sciences*, 2nd ed.; Elsevier: Amsterdam, The Netherlands, 2015; pp. 351–356.

[46] Rogers, M. (2003). *The role of criminal profiling in the computer forensics process. Computers & Security, 22(4),* p. 293.

[47] *Ibid.,* p. 294.

with an enormous speed and can be analyzed automatically thanks to the use of modern automation technologies. One of the examples of such technology is a solution called iACE, presented by the group of scientists headed by Xiaojing Liao. This tool can collect the IOC automatically and analyze the patterns between the intelligence sources, significantly reducing the amount of time spent on the online investigations[48].

Machine learning techniques can also be applied to the investigation of cybercrime in multiple ways. Raaijmakers discussed that the most common use of the machine learning and in particular an AI are the "suspect profiling, analyzing dark web money flows, child pornography detection and detection of anomaly in the surveillance"[49].


nmod:from
dobj
case
det
nsubj
det
compound
det
IOC token
Context term
✓ The Trojan downloads a file ok.zip from the server.
✓ All e-mails collected have had attachments clickme.zip.
✓ It contains a shellcode at offset 3344 that downloads and execute a PE32 file from the server.
• The malware does not modify AndroidManifest.xml in such a way.
• It's available as a Free 30 day trial download.
• Microsoft has already released an out-of-band patch MSMSv25-Patch1.zip

Pic. 14. Example of sentence based on IOC for further analysis by iACE (Liao; 2016).

Furthermore, AI can recognize the patterns in the behavior of the cybercriminal groups in order to investigate the illicit techniques used by them which can lead to the further detection of such patterns in the cybercrime scenes. One example of that is the ScamSlam project presented by Airoldi and Malin, which identifies the origins of the financial fraud with a use of unsupervised hierarchical clustering of the emails[50]. Besides, machine learning can also help to predict and, thus, prevent future cybercrimes, by analyzing the found crime trends.

Technology of blockchain can also be used in digital forensics as a method of proving the integrity and validity of the electronic evidence. Blockchain has an unchangeable nature, which means that any changes which were made to one of the blocks can be discovered. Saiedian

[48] Liao, X., Yuan, K., Wang, X., Li, Z., Xing, L., & Beyah, R. (2016). *Acing the IOC Game. Proceedings of the 2016 ACM SIGSAC Conference on Computer and Communications Security - CCS'16.*

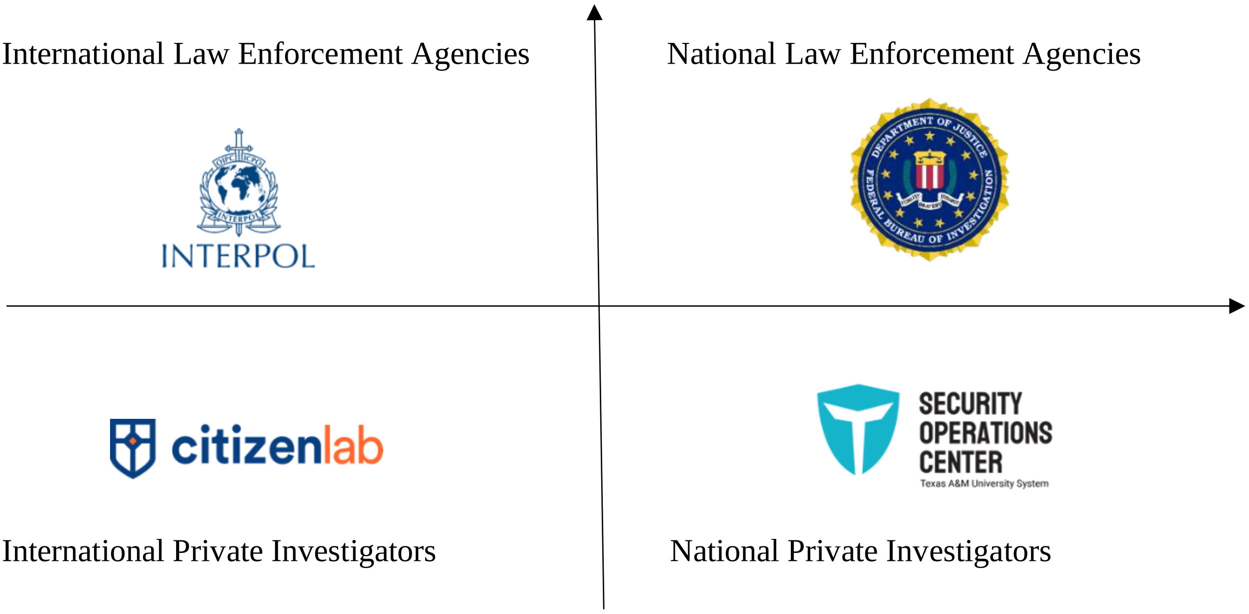
[49] Raaijmakers, S. (2019). *Artificial Intelligence for Law Enforcement: Challenges and Opportunities. IEEE Security & Privacy, 17(5),* p. 74.

[50] Edwards, M., Rashid, A., & Rayson, P. (2015). *A Systematic Survey of Online Data Mining Technology Intended for Law Enforcement. ACM Computing Surveys, 48(1),* p. 19.

discussed that this method allows the cybercrime investigators to prove that electronic evidence was collected and processed correctly, showing that the chain of custody for the evidence was untouched[51].

7. Possible Techniques in Prevention of the Cybercrimes

The feature of the cybercrime prevention is the close link to the cybercrime investigation. Cybersecurity and the cybercrime prevention techniques are mostly based on the information about the conducted cyberattacks and illicit activities in the cybercrime which were gathered because of the OSINT and DFINT activities or from the cybercrime itself. This is the reason of the necessity of close collaboration between the cybercrime investigation actors on all the levels: the cooperation between the private and public bodies, international and national legislative bodies, and head of states. The approaches to the cybercrime prevention match with the cybercrime investigation and divide to the criminological, technical, and legal ones.


International Law Enforcement Agencies
National Law Enforcement Agencies
INTERPOL
DEPARTMENT OF JUSTICE
FEDERAL BUREAU OF INVESTIGATION
citizenlab
SECURITY OPERATIONS CENTER
Texas A&M University System
International Private Investigators
National Private Investigators

Examples of the actors in the cybercrime investigation

7.1. Criminological Approaches on the Cybercrimes Prevention

One of the main criminological techniques in the prevention of cybercrimes is called a Situational Crime Prevention (SCP). SCP was created in the 1970s and originally helped to prevent and control “traditional” crimes. It is based on the position that the criminals act rationally while choosing the situation where they can commit a crime and thus the investigators can predict the

[51] Horan, C., Saiedian, H. (2021). *Cyber Crime Investigation: Landscape, Challenges, and Future Research Directions, Journal of Cybersecurity and Privacy 1, no. 4.* p. 580-596.

comfort situations for the crime to happen and prevent it in time. Before SCP was widely used, the leading criminological theory in crime prevention was the evaluation of the likelihood of participation in crime of a certain individual, based on the characteristics of the person who is supposed to commit the offense. Clarke argued that SCP, on its turn, evaluates the dynamics of the certain situations and helps to create the circumstances which exclude the possibility of commitment of crime[52]. He later discussed how the SCP can be presented using five strategies: “Increase the Effort,” “Increase the Risks,” “Reduce the Rewards,” “Reduce Provocations” and “Remove Excuses”[53].

Later the SCP use was extended to different types of crimes, including cybercrime. The aforementioned strategies can be used by the cybercrime prevention specialists and law enforcement agencies in order to decrease the attractiveness of the situations where the cybercrime could be committed or increase the effort which the cybercriminals make to receive a reward for a commitment of a cybercrime. In general, the motivation of the cybercriminal to commit cybercrime can be presented by the following reasons:

- Gathering Trophies (quest to become famous);
- General Mischief;
- Financial Gain;
- Revenge;
- Protest;
- Criminal Activity;
- Identity Theft;
- Forging Documents and Messages[54].

Thus, after the identification of the possible motivation, the law enforcement agencies can use the strategies of the SCP in order to prevent cybercrime in certain situations. For instance, Clarke proposed to apply the “Increase the Risk” SCP strategy to cybercrime, which uses the technique of “utilizing of place managers”[55]. This technique[56] involves place managers, who control the designated crime area, to increase the possibility of detection and apprehension of the

[52] Clarke, R.V., M.D. Krohn, A.J. Lizotte, G.P.Hall (Eds.). (2009). *Situational crime prevention: theoretical background and current practice, Handbook on Crime and Deviance. Springer New York, New York, NY,* p. 259-276.

[53] Clarke R.V., D.B. Cornish. (2003). *Opportunities, Precipitators and Criminal decisions: A Reply to Wortley’s Critique of Situational Crime Prevention, 16, Criminal Justice Press, Monsey, NY,* p. 88.

[54] Verma, M., Hussain, S.A., Singh K.S. (2012). *Cyber Law: Approach to Prevent Cyber Crime. International Journal of Research Review in Engineering Science and Technology, v. 1 (3).*

[55] *Supra* note 52.

[56] *Ibid.*

cybercrime. An example of such a place manager could be an Internet Service Provider or the person who moderates the social media platforms.

Sometimes, when the SCP is applied to the original crime, a situation called "crime displacement" occurs. Under "crime displacement" is understood the situation of relocation of crime from an initial target or a specific place because of crime-prevention efforts. However, as Finn and Stalans discussed, law enforcement agents' efforts on the prevention of pimping of online-solicited sex workers did not lead to the displacement of the pimps from advertisement sites like Backpage and Craiglist[57].

All in all, the main task of application of the SCP is to model the possible cybercrime threats. Thus, the main focus of the SCP is to make the cybercrime forestalled, which, unfortunately, cannot always stop the cybercrime from being committed. In order to reduce the possibilities of the cybercrimes to be comiited, there should be establishment of other preventive measures, including the technical and the legal.

7.2. Technical Approaches on the Cybercrimes Prevention

Technical measures helping to prevent the cybercrimes could be found, first of all, in the Standard/International Electrotechnical Commission (ISO/IEC) 27000-series which include the specification on how to provide technical protection for the information security of the companies' assets, like financial information, intellectual property and the personal data of the company and their clients.

For example, the ISO/IEC 270002 provide some measures to prevent the threats to the information security of the organizations, including cybercrime, by elaborating the situational use of technical and organizational measures[58]. Thus, Ho argues that SCP helps to prevent cybercrime by using the knowledge from computer science, criminology and cybersecurity[59].

On the national level, some states also elaborated technical standards for ICTs. For example, the EU starting from 2013 is issuing the Rolling Plan for ICT Standardization, which provides a link between the ICTs standardization techniques and the EU legislation and policies. The last version of the Rolling Plan for ICT Standardization was issued on 26 April 2022, which includes three main sectors of the ICTs development, among which is a cybersecurity/network and information security. Russia also issues the standardization instrument in the sphere of Information security, cybersecurity and privacy protection adopted on the level of the Commonwealth of

[57] Stalans, Loretta J., Mary A. Finn. (2016). *Understanding How the Internet Facilitates Crime and Deviance, Victims & Offenders, 11:4,* pp. 501-508.

[58] ISO/IEC 27002:2002.

[59] Heemeng, H., Ko R., Mazerolle L. (2022). *Situational Crime Prevention (SCP) techniques to prevent and control cybercrimes: A focused systematic review, Computers & Security, Volume 115.*

Independent States, containing technical measures in the sense of protection from cybercrime, called GOSTs.

The general technical measures on preventing cybercrime include the following one:

- establishment of the various areas of the security defense, including the security on the physical level and numerous internal and external security policies, constant monitoring for suspicious activity, etc.;
- introduction of the employers' level segregation and a "need-to-know" principle, meaning the access to the information should be established only on the basis of the need;
- establishment of the Removable device policy, e.g., all the removable devices (like USB) should be encrypted and tested for viruses before using with the other devices;
- introduction of the Cybersecurity Strategy of the company, establishing processes of preventing the cybercrimes and the techniques of recovering from them;
- organizing of the Cybercrime and Cybersecurity Awareness events, aiming on the education of the employees with standards of the security protection.

Most of the technical measures are implemented in order to protect assets of a company or individual from a cybercrime. Maras highlighted that under the "assets" is understood "something of importance of value, which include people, property, information, systems and equipment"[60]. Thus, companies' employees, personal data, intellectual property and private property fall under the category of assets.

Assets can have internal and external vulnerabilities. According to ENISA, internal vulnerabilities in the ICTs can include software code and design, security configurations and hardware[61]. For example, in 2018 a software bug in Monero's cryptocurrency provided an opportunity to the owners of Monero to exploit this vulnerability and double their cryptocurrency assets[62]. External vulnerabilities include, first, users who gained access to the companies' and individuals' assets. For example, the company's employees can open the attachment to the malicious email they received to the corporate email box and infect the corporate device with a virus.

Thus, internal, and external vulnerabilities lead in relation to the ICTs to the cyberthreats, which cause harm to the assets. Unfortunately, there is always a risk to face the cyberthreat while

[60] Maras M.-H. (2014). *Computer Forensics: Cybercriminals, Laws and Evidence, Jones and Bartlett*, p. 21.

[61] ENISA. (2017). *Hardware Threat Landscape and Good Practice Guide, Version 1.*

[62] Barth, Bradley. (2018). *Monero bug that doubled coin transfer amounts allowed attackers to steal from Altex.exchange. SC magazine*. Retrieved May 13, 2022, from https://www.scmagazine.com/news/cryptocurrency/monero-bug-that-doubled-coin-transfer-amounts-allowed-attackers-to-steal-from-altex-exchange.

working in cyberspace. This kind of risk can be defined as a probability of a threat and its consequences to materialize:

Risk = Probability x Consequences

The main procedures which help to deal with risk connected with the ICTs vulnerabilities includes building the technical and organizational management in the way which will mitigate the negative impact of the risk. Therefore, Risk Management is a prior mechanism which helps to identify, analyze, evaluate, and address the probability of security threats to the company or individual and to mitigate the consequences of such threats.

One of the most powerful instruments in Risk Management helping to prevent security threats is Threat Modeling. Basically, Threat Modeling is a set of procedures which is aimed at the protection of assets by identifying their possible vulnerabilities and threats and elaborating the possible countermeasures preventing them or mitigating the consequences of the threats. Threat Modeling involves multiple agents, including the developers, system administrators, analytics, and external consultants. It helps to increase awareness in the company in regard to potential threats, help to focus resources, coordinate the importance of protection from threats to the management and, finally, prevent the harm from the possible security threats.

7.3. Legal Approaches on the Cybercrime Prevention

Legal approach is focused on the measures regulating the risk mitigation and the cybercrime prevention. One of the instruments of preventive law is the General Data Protection Regulation (GDPR), which helps to minimize harm from the breaches of personal data leading to cybercrime. Cybercrime regulation is presented through laws which enable law enforcement agents to prevent cybercrime through the necessary measures and equipment. Thus, in the United States, the Communications Assistance for Law Enforcement Act contains a provision regulating an obligation of the Telecommunication Service Providers to provide an access to communications under lawful authorization for the government agencies[63].

In general, one of the main legal instruments in the prevention of cybercrime is a harmonization of cybercrime laws, international standardization of the requirements in regard to the electronic evidence and mutual legal cooperation in the cybercrime matters. This can be reached through elaboration of the unified cybercrime definition and jurisdiction on the international and national level will reduce a risk of possible exploitation of conflicts of cybercrime jurisdiction and lack of definition by cybercriminals for their own benefit. For example,

[63] 47 U.S.C., § 1001-1010.

introduction of the second additional protocol to the Budapest Convention, which is open to signing from the May of 2022, will hopefully improve cross-border access to the use of electronic evidence and enhance cooperation within the international society in cybercrime prevention[64].

UNODC in the Draft of Comprehensive Study on Cybercrime provided that national cybersecurity strategies also contain provisions on cybercrime prevention[65]. EUCPN states that Spain even elaborated a specific Crime Prevention Politics, highlighting the role of cybercrime prevention as a fundamental pillar in the fight against cybercrime[66]. The United Nations Guidelines for the Prevention of Crime highlight that the most important part of crime prevention is government leadership, which should be accomplished by international cooperation and partnership, especially in Public-Private relationships[67].

7.4. Approaches to Resolve the Cybercrime Investigation Challenges

As was mentioned above, there are several issues which can become challenges during the cybercrime investigation process. For example, cybercriminals by using the techniques of anonymity can engage in illicit activities without disclosure of their identity and location. However, anonymity can be used also by independent journalists or cybercrime investigators in order to analyze the behavior of cybercriminals and prevent the cybercrime.

One of the most popular techniques which helps to establish anonymity is the use of proxy services. A proxy service is an intermediary server that is used to connect a client with a resource and the server providing this resource. Proxy services can be anonymous and, thus, they hide users' identity by masking their IP address and replacing it with another one, which cannot identify a specific user. Anonymity networks, including the aforementioned Tor, Freenet and the I2P can not only hide IP addresses, but also encrypt the traffic of the users.

Another issue associated with anonymity is the creation of malware-infected zombie computers (botnets) and devices controlled through remote access (for instance, through the infected devices which have a backdoor providing a cybercriminal an opportunity to access these devices), which have different IP addresses and make it difficult to identify the initial source of a malware attack.

[64] CoEU. (2022). Second Additional Protocol to the Convention on Cybercrime.

[65] UNODC. (2013). *Comprehensive Study on Cybercrime.*

[66] EUCPN. (2018). *Crime Prevention Politics: Cybercrime, Child Sexual Exploitation, Credit Card Fraud, Crimes depending on ITCs.*

[67] *Guidelines for the Prevention of Crime*, annex to United Nations Economic and Social Council Resolution 2002/13 on *Action to promote effective crime prevention,* 24 July 2002, para. 3.

Which measures can be used to overcome the anonymity in the investigation of the cybercrime? One of the most prominent examples of such measures is cyber attribution. Cyber attribution is a process of tracking and identifying a person who is responsible for the cybercrime and the devices used for its commitment. For example, by using the traceback, cybercrime investigators can trace the illicit activities back to the source of the cybercrime. Thus, with the help of digital forensics, investigators can analyze the log files and by doing this extract some information about the committed cybercrime, like techniques, which the cybercriminal used during the attack, which can possibly identify the real IP address of the threat actor.

The allocation of IP addresses can be done through the registers, called Regional Internet Registries, which register and store a database of the IP addresses in the specific regions. Besides the IP addresses, Regional Internet Registries also contain the information associated with these IP addresses, like the name of the organization and contact information. For example, in the United States, the Regional Internet Registry is called an American Registry for Internet Numbers (ARIN) and the European IP addresses are coordinated by Réseaux IP Européens Network Coordination Centre (RIPE NCC). In Russia there are no integrated registries, however, the governmental body Roskomnadzor, which is responsible for the monitoring of Russian media contains a register of the IP-address for the companies, which activities are prohibited in Russia.

Furthermore, in order to identify the Internet Service Provider, which is associated with the certain IP address, cybercrime investigators can use the WHOIS query tool, provided by the Internet Corporation for Assigned Names and Numbers (ICANN). The WHOIS contains all the information provided by the users (individuals, companies, and governments) in regard to the registered domain names. The query tool inside the WHOIS can be useful during the cybercrime investigation as it contains the contact information of the users associated with certain IP addresses. Since the introduction of GDPR, access to the WHOIS instruments have been impacted, however, it is still widely used during cybercrime investigation. After the successful identification of the Internet Service Provider who provided access to the certain IP address, cybercrime investigators can make a request to this Internet Service Provider to identify the user using this IP address. This request should be accompanied with appropriate legal documents, usually, the court order or subpoena (for the United States).

The COVID-19 pandemic provided multiple challenges to the cybercrime investigators. This happens due to the numerous factors: unprecedented surge of the cybercrime cases (for example, only in the United States the growth of the registered cybercrime cases was more than 50% in 2020 in comparison to 2019), introduction of the “new reality” for people who started to do all their work and private activities online and introduction of the new healthcare services which were exploited by the cybercriminals. Law enforcement bodies all over the world needed to adopt strategies responding to the new challenges of cybercrime spreading. For example, Europol has straightened the campaign on the increasing of the cybercrime awareness and provided more resources and capacities to Member States and partner law enforcement authorities in the fight against cybercrime and cybercrime prevention. The Department of Justice in the United States also supported law enforcement bodies by counter the multiple healthcare fraud activities in cyberspace, including the issuing of the fake vaccination card and stealing of the Pandemic Unemployment Assistance, described in the previous parts.

Conclusion

The number of the committed cybercrimes growth significantly on the year basis and the cybercriminals are constantly exploiting the informational development of the world in their own benefit. These provide multiple challenges to the cybercrime investigation, which must be quickly adopted in order to comply with the spread of cybercrime and emergence of new types of cybercrime.

Investigation of cybercrime imposes many challenges on the actors. These challenges cover all three aspects of cybercrime: criminological, technological, and legal. However, the development of the technologies provides cybercrime investigators the possibilities to overcome the challenges. In short, these challenges can be presented in the following way:

Type of Challenges	**Technological Challenges**	**Legal Challenges**	**Ethical Challenges**
Lack of Best Practices in the Field of Cybercrime Investigation	Methodological (no unified techniques on conduction of the cybercrime investigation)	Methodological (no unified rules on work with digital evidence)	Challenges regarding the criminal profiling
Challenges Regarding the Data Gathered During the Cybercrime Investigation	The quality and the quantity of the collected data	The eligibility of the collected digital evidence (personal data issues)	The character of the received digital evidence (e.g. ethical issues of the information from honeypots)
Lack of Knowledge and of Qualified Human Resources	Lack of technical knowledge	Lack of legal definitions (no definition of the "cybercrime", no unified rules on the	Lack of the ethical and moral codes in the conduction cybercrime investigation

		establishment of cybercrime jurisdiction)	
Peculiarities of the Cyberspace	Anonymity (it is hard to track the cybercrime actor due to use of VPN and other anonymity techniques)	Anonymity (due to the problematic tracking of the cybercriminal, the issues regarding the personal data could arise)	Anonymity (biases regarding the identity of the cybercriminal, e.g. his nationality and profession)

Table 2. Challenges of The Cybercrime Investigation

Cybercrime investigation techniques have significantly developed through the last few years. This happened mostly due to the wide development of the AI and Big Forensics Data, which help not only to provide cybercrime investigation faster but also to avoid the mistakes during the investigation while choosing not eligible investigation techniques. For example, the processing of personal data with the automated tools helps to mitigate the risks linked with unauthorized use of the personal data, which can be helpful while analyzing the digital evidence during the cybercrime investigation, including, for instance, the information from honeypot.

COVID-19 pandemic also put the numerous challenges before the cybercrime investigators. This concerned an enormous growth of the number of the cybercrime, due to multiple factors, starting from the transition of most of the activities to online and the financial crisis, which is traditionally associated with the spread of criminal activities, especially, in the financial sectors. Nevertheless, due to the development of the investigation techniques and the raising of the cybercrime awareness, there is a great probability that the continuous growth of the number of cybercrimes can be stopped.

Thus, the technical measures using for the investigation and prevention of the cybercrime are continuing to improve. For example, the technique of cyber attribution techniques which can help to allocate the IP address of the cybercriminal has developed in the recent years and has adopted in the way which allows investigations to track the IP addresses even it was masked with the use of VPN servers and proxy.

Criminological trends in the cybercrime investigation also shows the progress. The leading approach in the cybercrime prevention is now the Situational Crime Prevention, which was borrowed from the “traditional” crime. The cybercrime investigation is now based on the digital forensics techniques which are developed under the practical use by both the law enforcement agencies and the private cybercrime investigators.

However, the legal approach, including the using of international and national law and the soft-law instruments, like cybersecurity strategies, should be considered as the primary source in the regulation of the cybercrime investigation and prevention management. Unfortunately, the existing legal instruments, including the Budapest Convention which was established to demolish the difficulties in the fight against cybercrime on the international level, still do not contain sufficient mechanisms helping to develop the international collaboration in the fight against cybercrime. The lack of the cybercrime definition and the problems regarding the establishment of the jurisdiction of the cybercrime turn the investigation into "gray zone" which can be used by the cybercriminals.

Despite the development of the technical and criminological instruments, the cybercrime investigation and prevention seem incomplete with a weak legal regulation of these fields. Thus, the international and national legislative bodies must elaborate the way of the development of new legal instruments or improvement of the existing one, which could help to solve the lack of definition problem. This approach can also influence the problems in the ethical and technical fields, mentioned in the Table 2. Thereby, the author believes that the international cooperation regarding the elaboration of legal instruments will help to avoid legal vacuum and is the main way of control of the cybercrime spreading and holding the cybercriminals accountable for their illegal actions.

Bibliography

Barmpatsalou, K., Cruz, T., Monteiro, E., & Simoes, P. (2018). *Current and Future Trends in Mobile Device Forensics. ACM Computing Surveys, 51(3).*

Barth, Bradley. (2018). *Monero bug that doubled coin transfer amounts allowed attackers to steal from Altex.exchange. SC magazine.* Retrieved May 13, 2022, from https://www.scmagazine.com/news/cryptocurrency/monero-bug-that-doubled-coin-transfer-amounts-allowed-attackers-to-steal-from-altex-exchange.

Caianiello, M., Camon, A. (Eds.). (2021)*, Digital forensic evidence. Towards common European standards in antifraud administrative and criminal investigations, Wolters Kluwer.*

Caviglione, L., Wendzel, S., & Mazurczyk, W. (2017). *The Future of Digital Forensics: Challenges and the Road Ahead. IEEE Security & Privacy, 15(6),* p. 14.

Clarke R.V., D.B. Cornish. (2003). *Opportunities, Precipitators and Criminal decisions: A Reply to Wortley's Critique of Situational Crime Prevention, 16, Criminal Justice Press, Monsey, NY,* p. 88.

Clarke, R.V., M.D. Krohn, A.J. Lizotte, G.P.Hall (Eds.). (2009). *Situational crime prevention: theoretical background and current practice, Handbook on Crime and Deviance. Springer New York, New York, NY,* p. 259-276.

CoEU. (2022). Second Additional Protocol to the Convention on Cybercrime.

Dark Web Price Index 2022 - Dark Web Prices of Personal Data. Privacy Affairs. (2022, March 16). Retrieved May 12, 2022, from https://www.privacyaffairs.com/dark-web-price-index-2022/.

Edwards, M., Rashid, A., & Rayson, P. (2015). *A Systematic Survey of Online Data Mining Technology Intended for Law Enforcement. ACM Computing Surveys, 48(1),* p. 19.

ENISA. (2017). *Hardware Threat Landscape and Good Practice Guide, Version 1.*

ENISA. (2019). *Introduction to Network Forensics.*

Eriksson, J., & Giacomello, G. (2014). International Relations, Cybersecurity, and Content Analysis: A Constructivist Approach. The Global Politics of Science and Technology - Vol. 2.

EUCPN. (2018). *Crime Prevention Politics: Cybercrime, Child Sexual Exploitation, Credit Card Fraud, Crimes depending on ITCs.*

FBI. (2020, 2021). *The Internet Crime Report*, p. 3.

Freeze, D. (2020, November 9). *Global cybercrime damages predicted to reach $6 trillion annually by 2021*. Cybercrime Magazine. Retrieved May 5, 2022, from https://cybersecurityventures.com/annual-cybercrime-report-2020/.

Giacomello, G. & Siroli, G. P. (2016). *War in Cyberspace*.

Guidelines for the Prevention of Crime, annex to United Nations Economic and Social Council Resolution 2002/13 on *Action to promote effective crime prevention*, 24 July 2002, para. 3.

Heemeng, H., Ko R., Mazerolle L. (2022). *Situational Crime Prevention (SCP) techniques to prevent and control cybercrimes: A focused systematic review, Computers & Security, Volume 115.*

Horan, C., Saiedian, H. (2021). *Cyber Crime Investigation: Landscape, Challenges, and Future Research Directions, Journal of Cybersecurity and Privacy 1, no. 4.* p. 580-596.

IBM. (2021). *Cost Of a Data Breach Report.*

Jang, Y. (2009). *Best Practices in Cybercrime Investigation in the Republic Korea, UNAFEI, Resource Material Series No. 79.*

Kisswani, N. M. (2011). *Telecommunications (interception and access) and its regulation in Arab countries. International Journal of Liability and Scientific Enquiry, 4(1), 44*.

Kommersant. (2021, November 11). *Failure of the Fake Vaccination Certificates.* Retrieved May 12, 2022, from https://www.kommersant.ru/doc/5066303.

Liao, X., Yuan, K., Wang, X., Li, Z., Xing, L., & Beyah, R. (2016). *Acing the IOC Game. Proceedings of the 2016 ACM SIGSAC Conference on Computer and Communications Security - CCS'16.*

Louw, D. Forensic psychology. In *International Encyclopedia of the Social & Behavioral Sciences*, 2nd ed.; Elsevier: Amsterdam, The Netherlands, 2015; pp. 351–356.

Manral, B., Somani, G., Choo, K.-K. R., Conti, M., & Gaur, M. S. (2019). *A Systematic Survey on Cloud Forensics Challenges, Solutions, and Future Directions. ACM Computing Surveys, 52(6).*

Maras M.-H. (2014). *Computer Forensics: Cybercriminals, Laws and Evidence, Jones and Bartlett*, p. 21.

Nazah, S., Huda, S., Abawajy, J. H., & Hassan, M. M. (2020). *Evolution of Dark Web Threat Analysis and Detection: A Systematic Approach. IEEE Access*, p. 5.

NIST. (2019). *Guidelines on Mobile Device Forensics.*

Quick, D., & Choo, K.-K. R. (2018). *Digital forensic intelligence: Data subsets and Open Source Intelligence (DFINT+OSINT): A timely and cohesive mix. Future Generation Computer Systems, 78*, p. 566.

Raaijmakers, S. (2019). *Artificial Intelligence for Law Enforcement: Challenges and Opportunities. IEEE Security & Privacy, 17(5),* p. 74.

Rogers, M. (2003). *The role of criminal profiling in the computer forensics process. Computers & Security, 22(4),* p. 293.

Sokol, P., Míšek, J. & Husák, M. (2017). *Honeypots and honeynets: issues of privacy. EURASIP J. on Info. Security 2017, 4.*

Stalans, Loretta J., Mary A. Finn. (2016). *Understanding How the Internet Facilitates Crime and Deviance, Victims & Offenders, 11:4,* pp. 501-508.

UNODC. (2013). *Comprehensive Study on Cybercrime.*

Verma, M., Hussain, S.A., Singh K.S. (2012). *Cyber Law: Approach to Prevent Cyber Crime. International Journal of Research Review in Engineering Science and Technology, v. 1 (3).*

Zetter, K. (2015, August 18). Hackers finally post stolen Ashley Madison Data. Wired. Retrieved May 12, 2022, from https://www.wired.com/2015/08/happened-hackers-posted-stolen-ashley-madison-data/.