Analysis of cybercriminals and where they fall on the spectrum of crime

Arbnora Miftari
Informatics
University of Tetovo
Tetovo, North Macedonia
a.miftari319026@unite.edu.mk

Shkurte Luma-Osmani
Informatics
University of Tetovo
Tetovo, North Macedonia
shkurte.luma@unite.edu.mk

Florim Idrizi
Informatics
University of Tetovo
Tetovo, North Macedonia
florim.idrizi@unite.edu.mk

***Abstract*—Analysis of published papers on criminal behavior raises questions about whether even the nature of cybercrime leaves room for the usual characteristics that show up in other types of criminals. This issue provides enough basis to consider a descriptive and quasi-experimental research aimed only at cybercriminals, which is also the aim of this paper. Taking into account the fact that there are almost no papers published on the same subject, the methods of this research are based on the gathering and analysis of raw data - videos and interviews of various cybercriminals, some under their real identity and others using pseudonyms. The observed characteristics will be compared with those of other types of criminals and with each-other, in an attempt to distinguish between causes and correlations in personality, social, economic and possibly other external and internal factors.**

Keywords—cybercrime,cybercriminal,criminal psychology, black hat hacking, white hat hacking, bug hunter, bug hunting, social engineering

I. Introduction

Out of all phenomena that have been studied in individuals or groups, crime continues to have the higher priority. Over the years there has been a great number of papers published on analysis and categorization of behaviours that can lead to criminal activity. The success has been so great, that now psychologists and detectives are trained on what to be aware of in their work.

However, when we take a look at the nature of cybercrime, there is almost no room for the usual "guidance manual". Aggressivity, for example, is a trait that is often present in many types of antisocial disorders, but it would be hugely disadvantageous to a cybercriminal, especially if the type of cybercrime is of such nature where patience and stubbornness are the main ingredients for success. Also, usually programmers or the DevOps team is not concerned about ethical issues in Developing [34].

II. Previous Works

In August of 2021, International Journal of Environmental Research and Public Health published a systematic review [2] using full text articles and research with at least 20 respondents, each one published at least in or after 2016, in an attempt to find the link between individual personality traits and criminal behaviour. The conclusion was that through this review, it is transparent that major personality traits such as psychopathy, low self-control, and a difficult temperament can be measured using various scales/inventory or secondary data. Thus, it is suggested that the interventions that aim to reduce the risk of criminality should begin during the early childhood stage since some of the existing evidence agrees that youths usually start engaging in criminal activities after reaching the age of 15 years old. Moreover, the identification of personality traits regardless of gender is also crucial to initiate appropriate preventative strategies for vulnerable groups such as children, at-risk youths, and adolescents."

An individual with low self-control and difficult temperament can grab something from the store in the heat of the moment, and would be impossible to be reasoned with when confronted, but it is difficult to believe that such an individual can spend hours, weeks or months of trial and error in his attempts to find system vulnerabilities.

An exception from the earlier systematic collection and other studies of the same nature will be James Oleson's "Criminal Genius" [1]. Oleson points out a huge flaw in many studies of criminal behaviour: They mostly take data from already convicted criminals. What about the ones who never get caught? He and his team published a questionnaire that was filled anonymously from hundreds of people, 44 of which accepted follow-up interviews.

Their findings were quite the revolution: Many individuals confessed to numerous crimes that were never reported. Upon further interrogation and psychological analysis, it was found that all of them had extraordinarily high IQs (130+). So, the relationship between crime and IQ that was previously believed to be linear, now had a parabolic shape. In Layman's terms, most crimes were committed either by people with really low or really high levels of intelligence, but the difference was that the second group hid their traces very well.

The characteristics of these high IQ criminals are as follows: "In addition to having higher IQ scores, the index group was proportionally more male, white, foreign, and unemployed. Fewer were heterosexual and proportionately more were separated, divorced, or living with a partner. They were older, were better educated, earned more, and were less religious. They were significantly more likely to report suffering from a mental illness, and a larger percentage of those who suffered from a mental illness also received mental-health treatment... Females had higher than average measures of addiction and although males more closely resembled controls than prisoners on a scale for criminality, they had higher criminality scores. Respondents had lower than average measures of extraversion, impulsiveness, and empathy. Males had lower than average measures of addiction but higher than average lie scores, suggesting potential dissembling on the test, while females had lower than average lie scores."

What we want to point out about this study is the fact that the people that accepted follow-up interviews in person were mostly older in age, ranging from 70 years old and up. No 20-

978-1-6654-9058-0/22/$31.00 ©2022 IEEE

year-old risked getting their identity known, for obvious reasons. Keeping this in mind, the collected audience was raised in a time period where they experienced WWII and also were subject to the cruel ways people punished homosexuals, which leaves very little room for surprise in the conclusion that a lot of them suffered from mental illness and very few were heterosexuals. Although there are multiple studies on cybercrime, few of them aim to understand the psychology of the offenders, which is understandable considering the fact that right now it is more crucial to understand the types of cybercriminal activity and its distribution by nationality, age and gender. However, a recently published paper [3] may show that this field of interest might prove to be very valuable.

This new study, done on Dutch youths in secondary or tertiary education (with ages between 12 and 25), who were following ICT programs, tracks, or courses, revealed that although many of them had committed cybercrimes, they did not display the expected characteristics of a cybercriminal nor were they affected by factors that are stereotypically associated with such offenders, e.g., knowledge of computers, academic failure, gaming, age, etc.

TABLE I. EFFECT OF VARIOUS FACTORS IN CYBER-DEPENDENT DELIQUENCY

Cyber - dependent delinquency	
Individual factors	***Environmental factors***
-Age + Low self-control + Good social skills + Computer addiction + ICT knowledge + Positive cyber- behavior	

[a.] Minus (-) = negative significant effect

[b.] Plus (+) = positive significant effect

TABLE II. EFFECT OF VARIOUS FACTORS IN CYBER-ENABLED DELIQUENCY

Cyber - enabled delinquency	
Individual factors	***Environmental factors***
-Age + Low self-control + Good social skills + Computer addiction + Positive cyber-behaviour	+Home alone -School satisfaction +ICT education satisfaction

[a.] Minus (-) = negative significant effect

[b.] Plus (+) = positive significant effect

TABLE III. EFFECT OF VARIOUS FACTORS IN TRADITIONAL DELIQUENCY

Traditional delinquency	
Individual factors	***Environmental factors***
-Age + Low self-control + Good social skills + Computer addiction - ICT knowledge + Positive cyber-behaviour	-Offline rules by parents -Online rules by school -School satisfaction +ICT education satisfaction

[a.] Minus (-) = negative significant effect

[b.] Plus (+) = positive significant effect

What is intriguing about these results is the fact that:

- A surprising overlap was found between cyber-delinquent behavior and positive cyber behavior, meaning that these pupils didn't always use technology for negative cyber behavior, or believed that their negative cyber behavior was justified.
- If pupil A confessed to having done something online that was illegal or unethical for fun, their friend, pupil B, who was observed to be a more of a hot-blooded kid, thought that A reacted that way online because he was provoked. This raises the concern that young people, unconsciously, tend to identify with their peers as much as possible, meaning that they are also more susceptible to justifying their friends' behaviors in order to feel connected to them.

The interesting dichotomies include the fact that many of these children were not socially withdrawn, but seem to have little clue about the actual cyber behavior of their friends, and the fact that children that committed cybercrimes also used their skills to help their peers or online friends. They didn't show typical unethical traits. A slight set-back, however, is that in the list of cyber-negative behaviors were actions such as: lying about your identity online, creating accounts with a fake name and/or birthday, lying or faking personal information such as home address or phone number, etc. We found these criteria to be a bit too strict, as many people do these things, especially younger generations.

III. METHODS

To obtain a better picture on how these individuals think and behave, interviews of known cyber criminals will be analysed (if possible, several interviews/videos for each of them, recorded some time apart - preferably years apart). We will see how these people rank on the traits that were highlighted in the studies cited, namely:

- Signs of psychopathy/sociopathy
- Low self-control
- Difficult temperament
- Academic education
- Family situation
- Addiction
- Dishonesty
- Reported mental illnesses

They will also be checked for possible characteristics that show up frequently but are not listed above.

IV. RESULTS

Throughout the process, some surprising environmental factors popped up. 40% of individuals stated that many databases of citizen personal data existed all around the globe. America had already made this news public, with the explanation that during the World War many hackers worked with the government to attack opposing countries. Years after the war ended, these hackers, in order to make profit, sold their data.

So, if you want to call abroad with stolen identities and buy various products, you don't have to be knowledgeable in

computer science. Of course, it doesn't work most of the time, but with a long list, even 1/10th chance of success can add up to 10 000 successes. Scammers that used bought data did in fact exhibit some of the traits of general criminals, this list including traits of psychopathy, sociopath, dishonesty, low self-control, economic difficulties, etc. [8-11][13][25] In cybercriminals that used computer knowledge for hacking, these traits were not apparent. Only one cybercriminal had problems with addiction and mental illness [14-19].

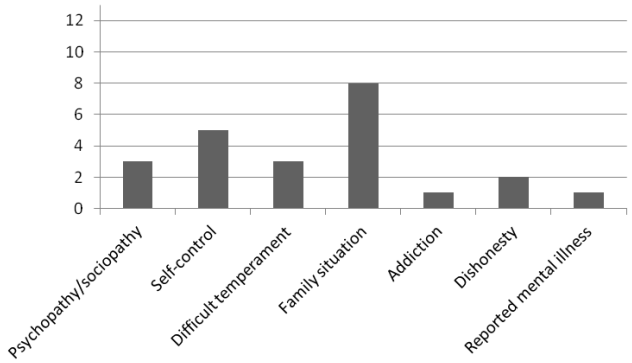

Fig. 1. How cybercriminals rank in the characteristics of traditional criminals

What is interesting is that out of all the individuals analyzed, those who started hacking later in life, which is roughly 38%, all reported either family problems or economic problems that affected them or their family [12][20-22][26-31]. They got involved in hacking by changing various jobs in an attempt to find a job that pays well and is satisfactory, or, they already worked in something IT related but were unsatisfied with either the pay or the job. From their reports, many black hat hackers start off as white hat hackers but start working illegally because they don't like the pay. The digital minister of Thailand (who is also subject of this study because she is a former hacker) keeps pushing for 7% of the government budget to go to white hat hackers, because of this phenomenon.

The hackers that started early in life usually did so by digging the libraries or internet for whatever they were curious at the moment [4-12][14-19][23-25][32-33]. They were approached by either family members, friends or online individuals that helped them develop their hacking skills and eventually ended up in closed communities of either white hat or black hat hackers. Many of these children/teenagers were not fully in control or aware of what they were doing. They started by using ready-made software or freaking with hardware components of electrical devices. Many stalked people online to gather information for social engineering, also in cyber stalkers often a recidivism is noticed [35]. Because of the fact that the people that helped them were other hackers that usually worked with stolen credit card information, they paid the young cybercriminals by having them make a list of things that they wanted that were then bought illegally and sent to them. On the other hand, those that were under the right influence, were incouraged to participate in various hacking competitions and gradually started working as white hat hackers, specifically bug hunters.

TABLE IV. SIMILARITIES AND DIFFERENCES BETWEEN CYBERCRIMINALS THAT STARTED EARLY AND LATE IN LIFE

Observed characteristics in cybercriminals	
Early in life (under 20)	***Late in life (over 20)***
- Curiosity - Persistance - Open to new experiences - Easily bored with routine - Easily influenced - Easily swayed	- Curiosity - Persistance - Open to new experiences - Easily bored with routine - Hard to change their minds - Think things through

It is important to note that, after these individuals did jail time, when they went out in society, they had a lot of trouble getting employed (because of their criminal record), so they ended up taking hacking or scamming tasks that pay them, even if in the past they had worked alone out of curiosity or for practical jokes. Although some of the subjects were socially awkward or had trouble socializing because of external reasons (frequent movement, academic success...), they don't seem to have a problem when making friends that indulge in similar cyber activities, which implies that as these children grow into adults, they tend to form isolated groups of likely -minded people. The incredible danger in this lies in the fact that many of them, after facing difficulties in employment, will turn for help to acquaintances in these communities, which only takes them further down the rabbit hole.

As these people grow up, they seem to become more alike. All of the participants regarded themselves as the ultimate judge for what is true and what is moral. Usually criminals know that they're committing a crime and get some sort of ego boost from doing something they shouldn't, or they blame their behavior on the economy, but cybercriminals seem to have a unique personal ethical system. When asked about their feelings and their take on their crimes, one group justified themselves saying they were harmless pranks, something they had to do to survive or they blatantly denied it was crime, because, in their perspective, they were doing something good, something heroic. The other group saw it as simple business, claiming that everybody does it so it's not a big deal. Many were careful to not get in trouble with the police by taking advantage of many gray areas in criminal law.

Depending on how early in life they started cybercriminal activities, these "moral systems" were either based on justifications and a bit of self-lies, or they were quite reasonable.

Although young cybercriminals were more easily swayed and did not question the motives of their friends, in general all cybercriminals got involved in the world of cybercrime by the help of people they knew, or people that they met online while surfing the internet out of curiosity. An important point to make is the fact that, as also illustrated in fig.2, white hat hackers were less isolated socially and therefore more susceptible to the influence of their families and/or real-life friends, whereas black hat hackers often got involved in online communities where they met other, already experienced black hat-hackers. The last group also had very little to say about their relationships with their families, indicating that they were, at best, not close with family members and didn’t share much with them.

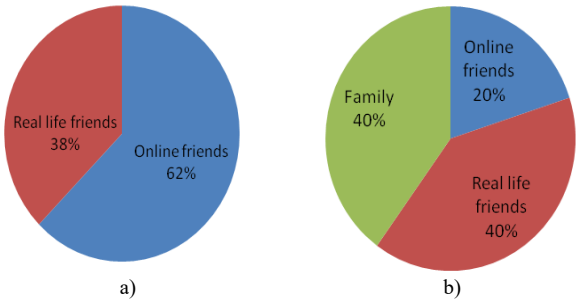

Fig. 2. a) People that influenced black hat hackers; b) People that influenced white hat hackers

V. Study Limitations

Although the sample frame includes individuals from various backgrounds and ethnicities: American, Australian, Turkish, Swedish, Chinese, Taiwanese, Japanese and Italian, the criteria for the videos that can be chosen made it extremely difficult to reach the number that was expected in the beginning, still, the total number of videos and subjects reaches the minimum required for statistical analysis (10 to 30 observations).

VI. Summary

Study results reveal that cybercriminals that were analysed in this process barely exhibited any of the listed traits of stereotypical criminal behaviour, with the exception of those that were doing illegal cyber activity using leaked and stolen data or readymade software. Although not asocial, many to all of their close friends were people knowledgeable and experienced in cybercriminal activities. They all had their own internal logic system that they used to determine whether what they did was right or wrong.

It is plausible to consider that what made a difference lied not as much in the personality traits as it did in the socio-economic factors. Children that had adults that they trusted were more likely to be encouraged to find legal ways of making a living by hacking, whereas children that did not share much with family and friends were likely to end up getting close with anonymous criminals online. Even as adults with huge economical disadvantages, they did start out as white hat hackers, and what would make a difference was how well informed they were by friends, company, news etc. about the road that they were about to take and how isolated they were from society.

Acknowledgment

This paper was finalized with the help of our colleague Shqipe Kaso, who helped diversify the sample frame by searching for and translating chosen interviews from Turkish to English. Special gratitude goes to the University of Bahrain for its motivation and support in making this research better and also giving it a chance to reach other academics and possibly spark their interest. Lastly, we are grateful to all the colleagues, friends and family members that were interested in the subject and offered their ideas for optimizing the research methods and also providing information on hacking cases they had heard of from documentaries or TV programs that could be of use in the gathering of the initial sample of data.

References

[1] Oleson James C. 2017. Criminal Genius : A Portrait of High-Iq Offenders. Oakland California: University of California Press.

[2] Tharshini, N. K., Fauziah Ibrahim, Mohammad Rahim Kamaluddin, Balan Rathakrishnan, and Norruzeyati Che Mohd Nasir. 2021. "The Link between Individual Personality Traits and Criminality: A Systematic Review" International Journal of Environmental Research and Public Health 18, no. 16: 8663

[3] Weulen Kranenbarg, M., van der Toolen, Y., & Weerman, F. (2022). Understanding cybercriminal behaviour among young people: Results from a longitudinal network study among a relatively high-risk sample. Amsterdam: VU University Amsterdam/Netherlands Institute for the Study of Crime and Law Enforcement.

[4] 60 Minutes. Julian Assange: The 2011 60 Minutes Interview. (Apr 12, 2019). Accessed: Jan 29, 2022. [Online Video]. Available: https://www.youtube.com/watch?v=Ubknv_CxSUY

[5] Journeyman Pictures. In Conversation With Julian Assange (2011). (Aug 8, 2016). Accessed: Jan 29, 2022. [Online Video]. Available: https://www.youtube.com/watch?v=AL76-VvMUH0

[6] 60 Minutes Australia. Wikileaks founder Julian Assange talks about escaping embassy (Oct 16, 2018). Accessed: Jan 29, 2022. [Online Video]. Available: https://www.youtube.com/watch?v=5Sp5IY9jZ_8

[7] World Ethical Data Forum (WEDF). WikiLeaks Founder Julian Assange's Last Interview Before His Arrest in London. (Feb 20, 2020). Accessed: Jan 30, 2022. [Online Video]. Available: https://www.youtube.com/watch?v=5Xh-GweVBUo

[8] Talks at Google. My Adventures as the World's Most Wanted Hacker | Kevin Mitnick | Talks at Google. (Sept 13, 2011). Accessed: Jan 31, 2022. [Online Video]. Available: https://www.youtube.com/watch?v=aUqes9QdLQ4

[9] Fox 5 New York. INTERVIEW: Former Hacker Kevin Mitnick. (Feb 17, 2015). Accessed: Jan 31, 2022. [Online Video]. Available: https://www.youtube.com/watch?v=oadw4y4zSI4

[10] Kevin Mitnick Sample Speaking Clips and Hacks You'll See Live. (Jan 23, 2017). Accessed: Jan 20, 2022. [Online Video]. Available: https://www.youtube.com/watch?v=7KCMK-LY-WM

[11] MitnickSecurityCom. Interview with renowned hacker Kevin Mitnick. (Apr 3, 2018) Accessed: Jan 20, 2022. [Online Video]. Available: https://www.youtube.com/watch?v=LaypU4qAuYw

[12] Soft White Underbelly. Hacker interview-Gummo (Dec 10, 2020). Accessed: Jan 23, 2022. [Online Video]. Available: https://www.youtube.com/watch?v=g6igTJXcqvo&t=1279s

[13] djvlad. Dzmitry Naskavets on Being a Cyber Criminal, Extradited to US, Prison Time (Full Interview). (Jul 13, 2021). Accessed: Jan 25, 2022. [Online Video]. Available: https://www.youtube.com/watch?v=3YDSxvaiyiw

[14] techtv. tss adrian lamo. (2011). Accessed: Jan 27, 2022. [Online Video]. Available: https://www.youtube.com/watch?v=6oHAPMEKvdM

[15] Vito Tums. Interview Adrian Lamo by John Draper Part 1 of 4. (2010). Accessed: Jan 27, 2022. [Online Video]. Available: https://vimeo.com/14820971

[16] Vito Tums. Interview Adrian Lamo by John Draper Part 2 of 4. (2010). Accessed: Jan 27, 2022. [Online Video]. Available: https://vimeo.com/14845518

[17] Vito Tums. Interview Adrian Lamo by John Draper Part 3 of 4. (2010). Accessed: Jan 27, 2022. [Online Video]. Available: https://vimeo.com/14850830

[18] Vito Tums. Interview Adrian Lamo by John Draper Part 4 of 4. (2010). Accessed: Jan 26, 2022. [Online Video]. Available: https://vimeo.com/14863468

[19] Al Jazeera English. Manning 'endangered US security'. (Mar 13, 2011). Accessed: Jan 23, 2022. [Online Video]. Available: https://www.youtube.com/watch?v=-U-omBeZMxc

[20] DEFCON 20. Kevin Poulsen Answers Your Questions. (2012). Accessed: Jan 28, 2022. [Online Video].Available: https://www.youtube.com/watch?v=SKVnR91ed5g

[21] Stanford Center for Internet & Society. (Full Version) Kevin Poulsen. (2011) Accessed: Jan 28, 2022. [Online Video]. Available: https://www.youtube.com/watch?v=zLhBwQ_V3ic

[22] Bugcrowd. Inside the Mind of a Hacker: Interview with @Hateshape. (Dec 12, 2018) Accessed: Sep 15, 2022. [Online Video]. Available: https://www.youtube.com/watch?v=C0jXyfD6PIo

[23] HackerOne. HackerOne Hacker Interviews: @RachelTobac. (Oct 1, 2018) Accessed: Sep 15, 2022. [Online Video]. Available: https://www.youtube.com/watch?v=AUsdBRFEE8k

[24] HackerOne. HackerOne Hacker Interviews: @filedescriptor. (Jul 27, 2018). Accessed: Sep 15, 2022. [Online Video]. Available: https://www.youtube.com/watch?v=5y3Hn9Y4gOc

[25] Orkun Işıtmak. Hapisten Çikan Türk Hacker İle Röportaj! (Jun 19, 2020). Accessed: Sep 16, 2022. [Online Video]. Available: https://www.youtube.com/watch?v=BLl5o7yTxPo

[26] Hitachi Brand Channel. "The People of Hitachi" White Hat Hackers – Hitachi. (Feb 26, 2021). Accessed: Sept 18, 2022. [Online Video]. Available: https://www.youtube.com/watch?v=1hbLU0oUpaQ

[27] AJ+. The World's First Transgender Minister. (Oct 4, 2016). Accessed: Sep 18, 2022. [Online Video]. Available: https://youtube.com/watch?v=R3JynXd_7lA

[28] France 24 English. Audrey Tang: A hacker-turned-minister in Taiwan. (Nov 16, 2018). Accessed: Sep 18, 2022 [Online Video]. Available: https://www.youtube.com/watch?v=H7thfNIo_iw

[29] South China Morning Post. Meet Audrey Tang, Taiwan's first transgender cabinet member. (Jun 26, 2020). Accessed: Sep 18, 2022. [Online Video]. Available: https://www.youtube.com/watch?v=CYOzAKfCpbY

[30] Hack Club. Hack Club AMA w/ Audrey Tang: Full Interview. (Jun 10, 2020). Accessed: Sep 19, 2022. [Online Video]. Available: https://www.youtube.com/watch?v=GzvNyImykCI

[31] I. Chiu, *"Digital Minister Audrey Tang: Taiwan's "Genius" and Her Unique Past"*, nippon.com, https://www.nippon.com/en/japan-topics/g00837/digital-minister-audrey-tang-taiwan%E2%80%99s-genius-and-her-unique-past.html , (accessed Sep 20, 2022)

[32] Bugcrowd. Inside the Mind of a Hacker: Mathias Karlsson (Full Interview). (Sep 29, 2016). Accessed: Sep 20, 2022. [Online Video]. Available: https://www.youtube.com/watch?v=yT5omaPizpg

[33] HackerOne. HackerOne Hacker Interviews: Mathias Karlsson (@avlidienbrunn). (Jan 23, 2018). Accessed: Sep 20,2022. [Online Video]. Available: https://www.youtube.com/watch?v=8WjtSiE76XU&t=2s

[34] Skenderi, M., Luma-Osmani, S., Imeri, F., Ethics in DevOps, The attitude of programmers towards it, *Journal of Natural Sciences and Mathematics of UT*, pg. 69-85, Vol. 5, No. 9-10, 2020

[35] Luma-Osmani S., Ismaili, F., Pathak, P., Zenuni X. Identifying Casual Structures from Cyberstalking: Behaviours Severity and Association. *J. Commun. Softw. Syst.*, pg.1-8, Vol.18, No.1, 2022