

DOI: https://doi.org/10.48009/1_iis_114

Behind the screen: psychological motivations and mental health issues in cybercriminal behavior

Charley Tyrrell, *Robert Morris University, cptst101@mail.rmu.edu*

Peyton Lutchkus, *Robert Morris University, pglst259@mail.rmu.edu*

Abstract

Cybercrime has been rapidly increasing, which makes understanding the criminals behind these serious misconducts crucial. This research examines existing literature that details the connection between mental health issues and cybercriminal behavior. The psychology behind cybercriminal behavior can bring many insights about why these behaviors have become prevalent, and if there are any patterns that can be observed. Financial gain, ideological beliefs, and thrill-seeking help provide some explanation as to what motivates cybercriminals. Mental illnesses can also play a role in causing an individual to engage in online criminal behavior. Many well-known hackers and cybercriminals have been diagnosed with mental health disorders, showcasing the potential connection these two topics have. These illnesses may be critical in understanding the relationship between mental health and participating in cybercrimes. This relationship can work to provide new strategies to combat cybercrime as well as improve mental health support resources.

Keywords: cybercrime, motivations, psychology, mental health, cybercriminals

Introduction

In recent years, cybercriminal activity and different types of cybercrime have caused damage to organizations worldwide. The current technological landscape has given cybercriminals many tools to perfect their craft and advance their techniques to increase the success rate of attacks. To be able to combat cybercrime, it is essential to understand more about cybercriminals and their psychological aspects. This research aims to examine psychological motivations and incentives that drive individuals to engage in cybercrime. The relationship between mental health issues and criminal behavior can help identify patterns to determine the tendency to commit cybercrimes.

This research explores underlying psychological factors such as thrill-seeking, ideological beliefs and financial gain and their connection to an individual's desire to participate in online criminal activity. Narcissism, antisocial personality disorder, anxiety, depression, and other mental health conditions are common diagnoses seen among cybercriminals. A case study examines some of the most famous and well-known cybercriminals and their mental health conditions. Research in this area can assist in developing effective strategies to reduce cybercrime and enhance mental health support for at-risk individuals.

Background

Cybercrime results from our society's widespread use of the Internet (Jadhav et al., 2022). New and evolving technologies have rapidly increased the cybercrime rate worldwide. These crimes can have devastating results, such as destruction of data, unauthorized access to systems, altering sensitive information, etc. Cybercriminals have found new tactics to carry out successful attacks in recent years. Hacking, phishing, and scamming are just a few cybercrimes prevalent today. Hacking is an illegal entry into a computer that can result in losses. This crime can lead to significant data loss, unauthorized access, and data breaches. Phishing uses deceptive emails to trick users into clicking on malicious links or giving up personal information. This is classified as an online scam and a type of social engineering, costing billions of dollars worldwide. Online fraudsters or scammers may pretend to be someone else to gain access to private information. These crimes will only continue to increase as cybercriminals find new ways to combat cybersecurity techniques.

In the digital era, cybercrime has grown exponentially (ContentEngine LLC, 2024). It is crucial to understand cybercriminals, their motivations, and what tools they use. Cybercrime is challenging to investigate because these criminals operate behind a screen, rather than in conventional crime where they are visible and noticeable. It is often tough to catch and prosecute cybercriminals because their main goal is to remain undetected or anonymous. Cybercriminals often get their start on the internet, where they can utilize free resources to learn essential information needed to carry out attacks. They can also engage with other cybercriminals to gain more knowledge, expertise, and experience with cybercrime. Motivations often vary for different cybercriminals, with one of the most predominant being finances.

The psychological traits of cyber trolls provide insight into their motivations to become master manipulators of their victim's emotions within cyber settings (Sest et al., 2017). Online trolling is the deliberate provocation of others using deception and malicious behavior on the internet that results in conflict, emotional reactions, and miscommunications. Studies have shown that gender and dark personality traits are predictors of those engaging in this behavior. A study of 415 participants found that men are more likely to engage in online antisocial behaviors in comparison to women. Psychopathy and sadism were found to be positive indicators of cyber trolling.

Due to technological advancements, there is now a much higher risk for cybersecurity threats (Bada et al., 2023). Cybersecurity threats can impact all areas of a person's life, including business and government processes. To create solutions to cybercrime, there must be an understanding of the cybercriminals themselves and their psychological profiles. Through case studies of notorious cybercriminals, many similar traits and characteristics were found. Many cybercriminals report developing their advanced technological skills in the younger years of their lives while also experiencing boredom at school. Some of the most notable cybercriminals also report struggling in their teenage years, having poor social skills, and being diagnosed with Asperger's syndrome. Understanding a cybercriminals' psychological profile can help uncover their motivations and prevent cybercrime.

Forensic psychology is typically focused on violent criminal activity; however, most forensic psychology theories can be applied to cybercriminal offenses (Kirwan, 2012). Forensic psychology can be defined as the involvement of psychology in the court of law, but the field is vast. Most forensic psychologists work directly with offenders by completing assessments and offering counseling, but forensic psychologists also aid victims, juries, judges, and lawyers. Offender profiling is an extremely popular technique used by forensic psychologists that is extremely popular in the media. Offender profiling is a technique that identifies a criminal's prominent and significant personality and behavioral characteristics based on a

thorough analysis of the crime committed. Although offender profiling is traditionally applied to homicide and sexual assault cases, this technique can be incredibly effective when used in cases of cybercrime.

Examining cybercriminals through a psychological perspective can reveal possible explanations for cybercriminal offenses (Campbell et al., 2012). Social psychological perspectives focus on situational factors' influence on cybercriminal behaviors, such as how anonymity and reduced social context can contribute to an individual's likelihood of engaging in cybercrime. Research in personality psychology has revealed that cybercriminals are likely to have characteristics of antisocial and narcissistic personality disorders, which can contribute to the tendency to engage in criminal activity. Cybercriminals often fail to view their acts as harmful or illegal, sometimes blaming the system designers for not protecting their programs enough, which aligns with characteristics of antisocial personality disorder.

The internet provides a new mode of communication in which users can be anonymous, causing growing concerns about cybercrime threats (Perenc, 2022). The anonymous environment provided through the internet allows individuals to portray themselves differently than they do in real life, often demonstrating antisocial and psychopathic personality traits. Internet users who display traits of an antisocial and psychopathic personality are more likely to engage in cybercriminal acts. Users with these personality traits are also more likely to engage in cybercriminal acts that are harmful to their victims, such as cyber harassment. Trolling has also been linked to traits of sadism, psychopathy, and narcissism.

Many notable cybercriminals have reported having an autism diagnosis, leading to an assumed connection between an autism diagnosis and cybercriminal behavior (Brewer et al., 2021). Studies suggest that those on the autism spectrum may be more likely to participate in acts of cybercrime than the general population, but this remains unproven. Individuals on the autism spectrum may be more likely to engage in cybercriminal acts due to deficits in the theory of mind, which prevents them from understanding the severity of cybercriminal activity. Deficits in the theory of mind also put those on the autism spectrum at risk of being exploited by cybercriminals. There may be a connection between high levels of autistic traits, rather than an official diagnosis of autism, and cybercrime.

There is little knowledge of the nature and extent of cybercrime, due to this group of offenders wanting to remain unseen or anonymous (Palmieri, 2022). Reinforcement sentiment theory has been used as a base theory for understanding what personality traits are related to motivations for certain behaviors. Cybercrime is often examined through the general theory of crime, in which multiple characteristics drive individuals to commit crimes. Low self-control, risk-taking tendencies, narcissism, introversion, and autism are some of the traits seen to increase the likelihood of an individual engaging in deviance.

The Space Transition Theory of Cybercrime aims to address the causes of these crimes through seven propositions (Jaishankar, 2007). A theory is needed to explain why cybercrime occurs in cyberspace. This theory explains the nature of an individual's conforming and non-conforming behavior in different spaces. It also argues that people behave differently in different spaces. Space transition involves the movement of someone from one space to another, for example, physical space and cyberspace.

Psychological Motivations for Cybercrime

Many reasons motivate individuals to engage in cybercrime, but the three most common motivations are thrill-seeking, ideological beliefs, and financial gain. These motivations can lure individuals into cybercrime, depending on what they are looking for and desire to gain. The types of cybercrimes committed also vary based on the cybercriminals' motivations.

Some cybercriminals are lured into crime by their desire for adrenaline, which aligns with the belief that some individuals commit crimes simply for the thrill (Brandefense, 2023). Cybercriminals who commit crimes for the thrill are motivated by the risk and excitement that criminal activity provides for them. Although they may receive financial gain from their criminal activity, that is not the main reason for their actions (Reynolds, 2024). They are searching for the thrill of outsmarting complicated security systems and making a name for themselves. These cybercriminals experience a rush, similar to those who participate in extreme sports, that influences them to continue their cybercriminal behaviors (Brandefense, 2023).

Cybercriminals may engage in criminal activity due to their own ideological beliefs. Cybercriminals committing crimes to leverage their ideological beliefs are often called hacktivists. Hacktivism is a form of non-violent cybercrime that aims to find solutions to civic issues or to reveal relevant information (Gawel, 2024). Hacktivists attempt to bring attention to political or social issues through their cybercriminal actions, much like activists in the physical space. Cybercriminals focused on their ideological beliefs are not seeking financial gain or adrenaline, instead they are hoping that their actions will lead to societal or political change.

Financial gain is the most notable motivation for cybercriminal behavior (Reynolds, 2024). Many cybercriminals begin engaging in cybercrime due to their desire to obtain money from their attacks. Those acting for financial gain often use ransom threats to receive millions of dollars in ransom payments (ContentEngine LLC, 2024). Cybercriminals often seek quick financial gain, focusing on hacking into bank accounts to receive a profit. Those motivated by financial gain are more likely to infiltrate systems for periods in order to complete more successful attacks.

Mental Health and Cybercriminals

Mental health is often at the center of discussion when evaluating individuals for their likelihood to engage in criminal behavior. The connection between mental health and cybercriminal behavior has been brought to light through multiple examples of cybercriminals with mental health disorders. Many disorders have been linked to criminal behavior, however, narcissistic personality disorder, antisocial personality disorder, depression, and autism spectrum disorder are the most notable among cybercriminals.

Narcissistic personality disorder is characterized by patterns of grandiosity, an extreme need for admiration, and a lack of empathy for others (American Psychological Association [APA], 2022). Individuals with narcissistic personality have a grandiose view of self, often believing that they are superior or have higher capabilities than their peers. These beliefs cause those with this disorder to have a very heightened sense of entitlement (Campbell et al., 2012). Entitlement has been noted as a characteristic of many dangerous cybercriminals, as they will seek revenge if they do not feel they have been appreciated. Individuals with narcissistic personality will also frequently rationalize in order to defend their behavior. An unidentified cybercriminal has stated that they view their actions as rising above everyone else. They view themselves as innovators attempting to bring their peers to new heights. Particular cybercriminals do not feel empathy for their actions, instead they believe others are misunderstanding their intent.

Antisocial personality disorder is defined as a persistent pattern of disregard for and violation of the rights of other individuals (APA, 2022). Cybercriminals have been noted to display these characteristics since they are often insincere and use charm or dishonesty to take advantage of their victims (Campbell et al., 2012). It has also been found that many cybercriminals fail to view their crimes as dangerous to others. Those engaging in cybercriminal activity will often blame others for their actions, stating that the software

designers are at fault for not protecting their designs. The anonymity provided through the internet provides the perfect setting for those with antisocial personalities to engage in criminal behavior (Perenc, 2022). Individuals with antisocial personality have been noted as being likely to commit cybercrimes, specifically cybercrimes that are harmful to their victims.

Depressive disorders are commonly characterized by the presence of sad and irritable moods, often seen accompanied by changes in an individual's ability to function (APA, 2022). An increase in irritable moods has been associated with a tendency to react to situations with outbursts, which can be linked to a likelihood of committing crime. It has been found that a diagnosis of a depressive disorder increases the odds of an individual being charged with a crime (Tayebi et al., 2024). Individuals suffering from depression have higher odds of being convicted of any type of crime, including severe crime. The connection between depression and the likelihood to commit crime can be compared to the likelihood of those diagnosed with narcissistic personality disorder to commit crimes. If an individual with depression is experiencing an increase in irritability, they could seek revenge against those they perceive to be causing those feelings, similar to those with narcissistic personality disorder engaging in cybercrime to get revenge on those who do not appreciate their abilities (Campbell et al., 2012).

Autism spectrum disorder is clinically defined as persistent deficits in communication and social interaction across multiple domains (APA, 2022). This disorder is associated with difficulty in maintaining and understanding relationships, which can put individuals at risk of being influenced to engage in cybercriminal activity (Brewer et al., 2021). Rather than there being a direct association between a diagnosis of autism spectrum disorder and cybercrime, it has been stated that perhaps specific traits can increase the likelihood of an individual's involvement in cybercriminal activity. Research has shown multiple similarities between those diagnosed with Asperger syndrome and cybercriminals (Campbell et al., 2012). These similarities include awkwardness in social interactions, a lack of empathy when engaged with others, and a fixation in technology.

Case Studies

When determining the relationship between mental health disorders and cybercrime, it is important to note the real-world scenarios that have shown this connection. This case study will examine some of the most famous cybercriminals, their crimes, motivations, mental health diagnoses, and other relevant information. This will help show how mental health disorders can contribute to an individual's engagement in cybercrime.

Gary McKinnon is known for infiltrating 97 NASA and U.S. Military computers to find critical information about UFOs (Naprys, 2023). His motivation for wreaking havoc on government systems was his obsession with finding out if the government was hiding information about aliens. McKinnon claims he did find evidence of aliens from the government systems but was eventually arrested in 2002 by the UK police. The U.S. government wanted McKinnon to be extradited so he could be charged over \$700,000 in fines after allegedly stealing hundreds of passwords, altering and deleting files, and making critical systems seemingly inoperable. The charges for these crimes meant McKinnon faced up to a 70-year sentence if extradited. An extensive legal battle was fought over the extradition for 10 years, as Britain refused to extradite Gary due to mental health issues and risk of suicide. McKinnon was later diagnosed with Asperger's syndrome, which is a condition that shows difficulties with social interaction and non-verbal communication along with repetitive behaviors. He also suffers from a depressive illness, which played a substantial role in the UK's decision not to extradite him to the U.S. (Frekelton, 2020).

Adrian Lamo is an infamous hacker known for multiple high-profile intrusions into major corporations (Blue Goat Cyber, 2024). Lamo conducted the 2002 breach of the New York Times' networks, where he accessed employees' personal details, contact information for high-level government officials, and inside information. Microsoft was another corporation Adrian targeted, along with U.S. government systems, Yahoo, and other social media platforms. Lamo faced legal repercussions after Chelsea Manning, a former Army intelligence analyst confided in Lamo about sensitive government information. He pleaded guilty to charges including felony computer crimes, including unauthorized access to computer systems. In 2004, Lamo was sentenced to two years of probation and paid fines for his charges. After being charged with his crimes, Adrian battled addiction and other mental health issues. When giving evidence during the trial of Chelsea Manning, Lamo revealed to the court that he had been diagnosed with several mental health conditions including general anxiety, major depression, and Asperger's syndrome (Pilkington, 2013). He stated that he takes medications for these conditions, and that these drugs had affected his memory at a few points in his life. Lamo also admitted to having a painkiller addiction at an earlier point in time.

Robert Tappan Morris is often called the first cybercriminal in the U.S. after releasing the first worm virus in 1988 (FBI.gov, 2018). This program was unleashed on the Internet from a computer at the Massachusetts Institute of Technology (MIT). Within 24 hours, over 6,000 out of the 60,000 computers connected to the Internet were infected. This worm had infected systems of multiple other prestigious universities and laboratories including Princeton, Stanford, Harvard, NASA, Johns Hopkins, and the Lawrence Livermore National Laboratory. After this incident had become public, the FBI launched an investigation and discovered Morris was behind the attacks.

In 1986, Congress passed the Computer Fraud and Abuse Act, which outlawed unauthorized access to protected computers. Morris was indicted in 1989 and found guilty a year later, making him the first individual to be charged under the 1986 law. His motivation for these crimes was to point out security issues and other system vulnerabilities (Bada et al., 2023). He had no malicious intent, but his actions slowed down and ruined some critical University resources. This sense of superiority and the act of crime in order to show a problem is linked to the trait of narcissism. In his earlier years, Robert Tappen Morris reportedly liked to work alone and showed traits of introversion, which can also be linked to online criminal behavior.

Julian Assange was known as Australia's most accomplished hacker in 1991 (Leigh et al., 2011). He was a computer programmer that founded WikiLeaks, a non-profit organization that publishes sensitive information leaks. Assange and two others also founded International Subversives magazine, which provided tips on "phreaking", an illegal way to break into telephone systems and make free calls. They frequently hacked computers and took down systems at Australia's National University. The same group of three targeted MILNET, the U.S. military's secret defense data network. When describing his motivations for these crimes, Assange stated he had an arrogance and desire to show off his computer skills (Bada et al., 2023). Julian was not very interested in school, had poor social skills, and a dry sense of humor. It is also reported that Assange disregarded people he did not necessarily approve of, had anger issues, and had swift mood changes. These traits of psychoticism, neuroticism, and extraversion indicate susceptibility to committing criminal behavior.

Some of the most famous cybercriminals have been diagnosed with mental illnesses, as seen above. Anxiety, depression, narcissism, addiction, and autism are some of the patterns identified among those who participate in serious online crimes. These disorders can play a part in determining what causes or increases the likelihood of someone committing crimes like those studied above.

Cybercrime Prevention

Cyber attacks and online criminal behavior have continued to evolve, with new tactics being used to cause serious damage worldwide (Institute of Data, 2024). The impact of these crimes displays the importance of robust prevention and intervention strategies needed to address the psychological aspects of cybercrimes. Psychology plays a crucial role in developing and implementing measures to improve the effectiveness of cybersecurity measures overall. The study of cybercriminals and their motivations help cybersecurity professionals formulate strategies to help combat online threats. The underlying psychological processes of a hacker's mindset prove to be very beneficial.

Understanding why cybercriminals choose to attack in the ways they decide can provide insights into their thought processes, which in turn can be used to help prevent attacks by anticipating their next moves. High levels of intelligence, narcissistic tendencies, and risk-taking behaviors are only a few of the many traits seen in cybercriminals. Many cybercriminals face mental health issues, including anxiety, depression, and more, that may play a part in the thought process behind engaging in these acts.

Behavioral interventions and better mental health support for at-risk individuals can potentially deter these criminal acts by addressing the psychological aspects that contribute to cybercriminal behavior. Receiving an accurate mental health diagnosis from a psychology professional can allow individuals to engage in appropriate treatment, which may positively impact the likelihood of them engaging in cybercriminal behavior. Exploring cybercriminals' motivations bring valuable insights into how or why they choose to attack. This understanding allows for better strategies to be implemented to prevent cybercrimes.

Conclusion

Cybercriminal activity has become increasingly threatening in recent years due to advancements in the technological realm. These advancements have given cybercriminals advanced tools to increase the severity of their attacks. To fight against the rising rates of cybercrime, it is essential that an understanding of the psychological motivations and incentives behind cybercriminals is built. This research examined the psychological motivations and incentives that lead individuals to engage in cybercrimes. Mental health can be used to examine the behavioral factors that predict an individual's tendency to commit cybercrimes.

This research explored psychological factors, such as thrill-seeking, ideological beliefs, and financial gain, and their influence on cybercriminal behavior. Connections between narcissistic personality, antisocial personality, depression, and autism spectrum disorder and the likelihood of engaging in cybercrime were also explored. Case studies of notorious cybercriminals were evaluated for psychological motives and mental health conditions. Limitations in this research exist due to a small number of case studies, making further research needed to develop strategies to prevent cybercrime and to provide adequate mental health support for those at risk.

References

- Bada, M., & Nurse, J. (2023, August 30). *Exploring Cybercriminal Activities, Behaviors and Profiles*. <https://arxiv.org/pdf/2308.15948>

- Brandefense. (2023, December 5). *The psychology behind cyberattacks: What motivates hackers?* <https://brandefense.io/blog/drps/cyberattacks-what-motivates-hackers/#:~:text=Thrill%2DSeeking:%20Much%20like%20adrenaline,can%20be%20an%20irresistible%20motivator.>
- Campbell, Q., & Kennedy, D. M. (2015). The Psychology of Computer Criminals. *Computer Security Handbook*. <https://doi.org/10.1002/9781118851678.ch12>
- FBI. (2018, November 2). *The Morris Worm*. Federal Bureau of Investigation. <https://www.fbi.gov/news/stories/morris-worm-30-years-since-first-major-attack-on-internet-110218>
- Freckelton, I. (2020). Autism spectrum disorder and suitability for extradition: Love v the Government of the United States [2018] 1 WLR 2889; [2018] EWHC 172 (Admin) per Burnett LCJ and Ouseley J. *Psychiatry, Psychology and Law*, 27(2), 181–191. <https://doi.org/10.1080/13218719.2020.1727645>
- Gawel, H. (2024, April 4). *Hacktivism*. Internet Policy Review. <https://policyreview.info/glossary/hacktivism>
- Inside the world of cybercrime: profile, motivations and tools of cybercriminals. (2024). *ProQuest*. <https://www.proquest.com/docview/3087658351/abstract?pq-origsite=summon&sourcetype=Wire%20Feeds&parentSessionId=FCEReLDI2Eh0vfcWTgfnY4h%2BZqeVwJ9bNUwrrp19Mc%3D>
- Institute of Data. (2024, July). Exploring the Psychology of Cyber Attacks: The Attacker's Mind | Institute of Data. <https://www.institutedata.com/us/blog/the-psychology-of-cyber-attacks/>
- Jadhav, S., Sonone, S., Singh Sankhla, M., Kamari, M., Kacker, P., & Kumar, R. (2022, December). *Psychological Influences of Cyber Crimes on Human Mind and Behaviour*. https://www.researchgate.net/profile/Mahipal-Singh-Sankhla/publication/380402545_Psychological_Influences_of_Cyber_Crimes_on_Human_Mind_and_Behaviour/links/663b35637091b94e93f93ee1/Psychological-Influences-of-Cyber-Crimes-on-Human-Mind-and-Behaviour.pdf?origin=publication_detail&tp=eyJjb250ZXh0Ijp7ImZpcnN0UGFnZSI6InB1YmxpY2F0aW9uIiwicGFnZSI6InB1YmxpY2F0aW9uRG93bmVxYWQiLCJwcmV2aW91c1BhZ2UiOiJwdWJsaWNhdGlvbiJ9fQ&__cf_chl_tk=vfKxg2F_NXsXUemlj206A2UvJ_f.5JPINDvza3SYQiI-1731606149-1.0.1.1-aQu9ABihzy78cN_GvOt6W2uuJTLj8EJMAS2qumntpi8
- Jaishankar, K. (2016). Establishing a Theory of Cyber Crimes. *Core.ac.uk*, 1(2). [oai:zenodo.org:18792](https://oai.zenodo.org/18792)
- Kirwan, G., & Power, A. (2012). *The Psychology of Cyber Crime: Concepts and Principles*. Google Books. https://books.google.com/books?hl=en&lr=&id=7OyeBQAAQBAJ&oi=fnd&pg=PR1&ots=rRoyAHOLFm&sig=jdFAzC_Bsnhvr3SzYwfvx_XMXgg#v=onepage&q&f=false
- Leigh, D., & Harding, L. (2017, November 26). *Julian Assange: the teen hacker who became insurgent in information war*. The Guardian; The Guardian. <https://www.theguardian.com/media/2011/jan/30/julian-assange-wikileaks-profile>

- Lim, A., Brewer, N., & Young, R. L. (2021). Revisiting the Relationship between Cybercrime, Autistic Traits, and Autism. *Journal of Autism and Developmental Disorders*, 53. <https://doi.org/10.1007/s10803-021-05207-1>
- Naprys, E. (2023, October 31). *The hacker who breached NASA to prove that UFOs exist* | Cybernews. Cybernews. <https://cybernews.com/tech/hacker-who-breached-nasa-trying-prove-ufo-existence/>
- Palmieri, M. (2022). *Decrypting Personality: The Effects of Motivation, Social Power, and Anonymity on Cybercrime* - ProQuest. Proquest.com. <https://www.proquest.com/docview/2724700785/fulltextPDF/DC71CDF8F9A948CCPQ/1?%20Theses&sourcetype=Dissertations%20>
- Perenc, L. (2022). Psychopathic personality disorder and cybercriminality: an outline of the issue. *Current Issues in Personality Psychology*, 10(4). <https://doi.org/10.5114/cipp.2022.114205>
- Pilkington, E. (2013, June 4). *Adrian Lamo tells Manning trial about six days of chats with accused leaker*. The Guardian; The Guardian. <https://www.theguardian.com/world/2013/jun/04/adrian-lamo-testifies-bradley-manning>
- Reynolds, A. (2024). *Profiling Cybercriminals: Behavioral Analysis and Motivations Behind Cybercrime Activities*. ODU Digital Commons. <https://digitalcommons.odu.edu/cgi/viewcontent.cgi?article=1094&context=covacci-undergraduateresearch>
- Sest, N., & March, E. (2017). Constructing the cyber-troll: Psychopathy, sadism, and empathy. *Personality and Individual Differences*, 119, 69–72. <https://doi.org/10.1016/j.paid.2017.06.038>
- Who Is Adrian Lamo? - Blue Goat Cyber*. (2024, February 25). Bluegoatcyber.com. <https://bluegoatcyber.com/blog/who-is-adrian-lamo/>