EasyChair Preprint

№ 15190

The Dark Web and Cybercrime: Identifying Threats and Anticipating Emerging Trends

Sheetal Temara

October 3, 2024

THE DARK WEB AND CYBERCRIME: IDENTIFYING THREATS AND ANTICIPATING EMERGING TRENDS

Sheetal Temara*
University of the Cumberlands, Williamsburg, KY
Email: stemara22276@ucumberlands.edu
ORC ID: *0009-0006-2221-6605*

ABSTRACT

Background/Objective: The Dark Web has played a pivotal role in the progress and sophistication of cybercrime. It provides an incubation network beyond the reach of traditional search engines where cybercriminals create and display exploit kits, offers illicit goods and services, and exchange confidential insider intelligence. Cybercriminals are extremely adept at selecting targets, applying tools to achieve their objectives, and minimizing red tape. The increasing sophistication of cybercriminals and the exponential rise of cybercrime against critical infrastructure underlines the necessity of identifying emerging threats. The objective of this research is to investigate the evolving threats within the Dark Web including crimeware-as-a-service and the integration of AI/ML into cyberattacks to inform risk management strategies and strengthen security measures.

Research Problem: The exponential rise in cybercrime against critical infrastructure reflects growing sophistication presenting a significant challenge to organizations and society. The motivation behind cybercrime is fundamentally driven by self-greed which has contributed drastically to the magnitude and changes in methods used by cybercriminals to enhance profitability. The impact of cybercrime on business organizations presents an adverse impact on society and carries significant risks for the progress of individuals and the world at large. As cybercriminals adopt new technologies and services such as crimeware-as-a-service, identifying emerging trends becomes crucial to developing proactive strategies for the detection and prevention of cyber threats.

Methodology: This research employs a systematic literature review approach to analyze emerging trends in cybercrime originating from the Dark Web. The review includes scholarly articles, news sources, and blog posts sourced from platforms like Google Scholar, IEEE Xplore, and various libraries. The key focus is to answer questions regarding the relationship between the Dark Web and cybercrime, accelerating cybercrime activities, and the benefits and implications of these new trends.

Results: Key findings of this paper range from the rise of crimeware-as-a-service attacks and the increasing use of artificial intelligence and/or machine learning capabilities by cybercriminals to automate attacks across various businesses and organizations are also propounded along with information related to entry points and cybercrime attack pathways. The emergence of sophisticated cybercrime techniques including ransomware-as-a-service, targeted attacks using AI and exploitation of IoT vulnerabilities are identified as critical trends. Social engineering, malware, and the rise of remote work have expanded the attack surface for cybercriminals.

Discussion: As the use of cybercrime continues to metamorphose, the identification of new threats and extrapolation of emerging trends is critical to investigate the challenges associated with the monitoring and detection of illegitimate activities on the Dark Web as well as for the establishment of proactive risk management strategies and implementation of robust security measures. The research highlights the transformation of cybercrime into a structured and scalable ecosystem driven by technological advancements and service-based attack models. Cybercriminals now leverage AI/ML increasing the sophistication and success of their attacks. The commoditization of cybercrime has enabled less skilled individuals to participate amplifying the volume and diversity of threats faced by organizations.

Conclusion: As cybercrime continues to evolve and adopt emerging technologies, organizations must remain vigilant and adaptable. The findings emphasize the need for proactive risk management, continuous monitoring of cybercrime trends, and robust security measures to mitigate the increasing threats originating from the Dark Web. Future research should focus on deeper exploration of AI-driven attacks and the development of more advanced countermeasures to safeguard critical infrastructure.

Keywords: Cybercrime; Dark Web; Cybercriminals; hackers; AI

1. INTRODUCTION

The Dark Web is a hub for illicit activity. It also provides services like botnets and zero-day vulnerabilities for lease. An accumulation of amenities concealed from standard internet users and web crawlers is known as the "Dark Web". The primary data available on the Dark Web is stolen data, drugs, illegal goods, counterfeit money, and weaponry, malware, hacking tools such as exploit and phishing kits, and illegal pornography but research has also exposed that there are many merchandise offerings related to cybersecurity including botnets that can be least, credentials for a variety of different organizations, and zero-day vulnerabilities. Inhabitance of the Dark Web includes nation states and cybercriminal organizations maturing and professionalizing their capabilities while bartering their stolen data and hacking services [1].

The exact magnitude of the Dark Web is challenging to estimate as most web properties are temporal in nature due to law enforcement, internet service providers (ISPs), and tension with rivals as well as self-enforced detection avoidance by taking the sites offline on purpose. The growth of the Dark Web has been massive as in 2012 there were only a few hundred websites which exceeded 100,000 websites in 2020 [3]. Of note is that most of the websites on the Dark Web are isolated islands with no links to or from other websites. The Dark Web can only be accessed with distinct software bestowing entry to networks that conceals the identity of the users as well as the supplier of the services [4]. The Dark Web is made up of web properties, marketplaces, message boards, and social media. Not only does the Dark Web provide anonymity, but it also conceals network activity and the information traded through it [6]. Groups of hackers make use of the Dark Web systems to distribute hacking utilities, file sharing, malware, compromised data, ransomware, and attack plans to discuss their activities and disseminate current relevant knowledge. The offerings in the Dark Web have evolved into service offerings such as ransomware-as-a-service (RaaS), malware-as-a-service (MaaS), phishing-as-a-service (PaaS),

Crimeware-as-a-service (CaaS) which demonstrates that cybercrime is transforming from a fad into a growing business empire.

The evolving service models have enabled anyone including lower-skilled criminals with Bitcoin to perform activities as a hacker [5]. The objective of the attack may not necessarily be direct monetary gain but the end goal may be to compromise the organization's infrastructure to steal information that in turn could be sold on the Dark Web. Currently, the business model is expanding to have professional branding and marketing promotions to make their products more appealing and increase their cash flow [8]. The more affluent cybercriminals offer customer support assistance with their products to provide a differentiator so that they attain a competitive advantage in the congested virtual marketplace. Within the Dark Web, cybercriminals also recruit personnel similar to a contemporary organization by using job postings and interviews but they need to exert caution to ensure the potential employee is not a disguised law enforcement agent [9].

TOR (The Onion Router) and I2P (Invisible Internet Project) networks are two of the most highly favored networks that facilitate propagating content on the Dark Web [10]. TOR was implemented in 2004 after the deployment of the relay network. At that point, TOR began to not only offer online anonymity to applications over cyberspace but also allowed the deployment of anonymous services over the Internet. The TOR Browser was created to facilitate safe web surfing in an anonymous fashion [20]. This browser transmits all web requests via the TOR network while cleansing all fingerprinting information from the transmitted data. The TOR browser fosters hidden services with hidden IP addresses to ensure anonymity between users and websites.

The Dark Web has expedited cybercrime's evolution into a versatile reputation aware business model by delivering an anonymous internet-accessible ecosystem that allows cybercriminals to cooperate, structure, increase their proficiencies, and form illegitimate business fronts. Criminal endeavors committed in a digital domain can be considered "cybercrime" [21]. The primary objective of cybercrime is to illicitly obtain as much as possible using the least amount of resources. Besides hacking, other varieties of crimes manifest into this realm. Initially, cybercrime was committed by hackers to achieve personal fame and increase their reputation and was not perceived as a source of income until the dotcom era in which the initial phase of cybercrime began from 1990 to 2006. The expansion of cybercrime has been enormous as reported between 2008 and 2021, there was a 207 percent growth in cybercrime activities resulting in damages reaching about $7 billion in 2021 which was being propelled by developing a cybercrime supply chain with enhanced professionalization and collaboration. Beginning in the 1980s, $6 trillion of destruction can be directly attributed to cybercrime and the amount of damages is expected to increase to $10.5 trillion by 2025 [26]. In 2020, 4.7 million cyber-attacks were declared in the United States in comparison to 1.5 million cyber-attacks in 2010 which is an approximate 300 percent increase in the total number of cyber-attacks [22].

The majority of victims originate from the healthcare, finance, government, education, and energy industries of G20 countries. As most people are reliant on groceries, apparel, and instruments supplied by firms connected to the Internet, any interruptions to these organizations'

operations could interrupt the supply chain resulting in regular people not having day-to-day essentials [23]. Monetary impact as a result of cybercrime can be colossal and extremely challenging to forecast or estimate. Similar to the advancement of genuine business, cybercrime is undergoing a similar growth period in which is experiencing progressive evolution to increase the return on investment. Cybercrime has been attacking organizations to increase payouts going back to 2018 as it continues to evolve its business strategy to a service-based paradigm. This has enabled cybercriminals to utilize multifaceted supply lines to facilitate attacks with plug-and-play elements [24]. The approach to cybercrime has transformed to be more methodical and focused. The cybercriminals are spending more time planning by concentrating on the selected target's architecture which will expand the effectiveness and multiply the monetary reward to increase their influence. The difficulty in securing critical information has been exacerbated due to the number of cyber-attacks that are occurring and the variety of cyber threats that are on the rise. For instance, RaaS has increased the number of ransomware attacks making this threat mainstream. As cybercriminals share their skills and expertise, the exploits are becoming increasingly more complex and detrimental [25]. The Dark Web with its developing environment enabling chats and online communities boosts reliable collaborations and fine deception. Cybercrime can showcase that companies have violated consumer privacy regulations during successful exploitation. The flowchart diagrams 1a and 1b illustrate how cybercriminals infiltrate organizations using various attacks amd services which lead to data theft, ransomware deployment, and monetary gain.

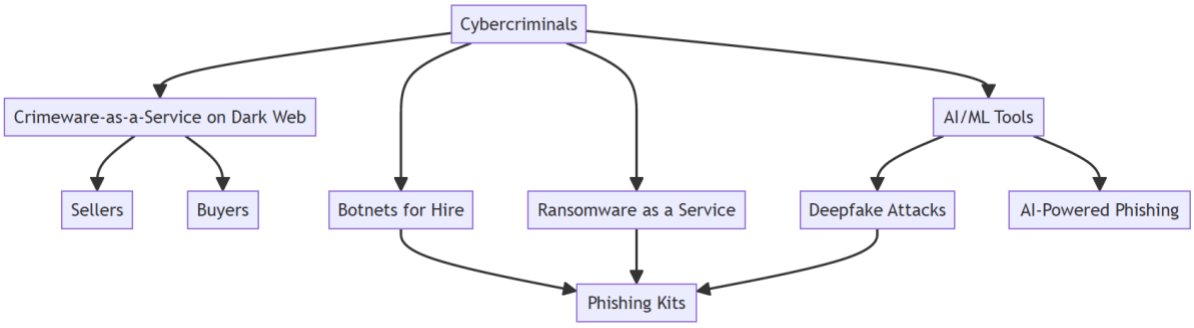

Figure 1a: Emerging Cybercrime Trends

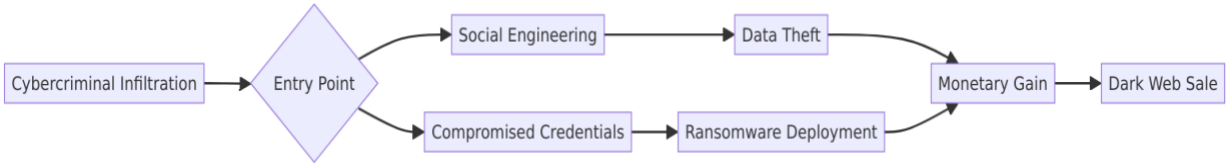

Figure 1b: Cybercrime Attack Pathways

There are four primary takeaways to understand regarding emerging cybercrime. One is that every attack needs an entry point into the target's infrastructure which renders control and access as primary requirements when executing cybercrime. One of the most common entry points

heavily favored by cybercriminals currently is social engineering. Another entry point that is popular is the use of compromised credentials which can be obtained on the Dark Web at a minimal cost [26]. A third entry point can be through the exploitation of existing weaknesses and vulnerabilities within software and infrastructure. The second takeaway from cybercrime is the commoditization of exploit kits decreases costs and at the same time provides an income source for cybercriminals who can lease specialized software for exploitation in parallel with allowing the malicious software authors to provide training and intricate instructions with the details needed to successfully execute the malicious software [27]. This demonstrated the maturation of the malware business model as cybercriminals are also transforming to bartering their knowledge and capabilities while no longer marketing their malicious utilities. It was identified by Wolf Security that the cost for 91 percent of marketed exploit kits was under $10, however, the pricing of tailored exploit kits varies from $1000 to $4000 [12]. The third takeaway is that in environments for cybercriminals, complex feedback tracking has been created so that suppliers and clients can track trustworthiness and client ratings. The final and fourth takeaway is that the cybercriminal communities in the Dark Web allow a place for collaboration between clients, suppliers, partners, and potential staff [28]. Cybercrime will continue to evolve as new threats and trends emerge [38].

2. LITERATURE REVIEW

The Dark Web is comprised of a combination of concealed services offering a range of illegal goods for sell from weapons and drugs to illegal pornography as well as cyber security related material including stolen credentials, zero-day exploits, and botnets that can be leased [2]. The Dark Web's dimensions and actions are challenging to measure and map due to outside influence from service provider monitoring, law enforcement investigations, and competitor manipulation [2]. It is noted that that Dark Web requires specific software providing anonymity for both the client and service provider to enable access [33].

Criminal activities and content including hacking utilities, cyberattack plans, malware, ransomware, and compromised confidential information including credentials plans are considered to be primarily hosted in the Dark Web [34]. Expansion can occur in cybercrime networks along with new paths for strategizing and executing cybercrime due to social network forums [35]. Access to the Dark Web conceals the client's information as well as the data traversing the network while requiring custom software to facilitate access [7].

Cybercrime as a business is continuing to transform similarly to genuine organizations to enhance efficiencies by providing as-a-service offerings. This new angle for crime related business not only commoditizes malware providing an income stream to those threat actors with expertise, but also provisions more advanced attacks to a broader spread of individuals who are not highly skilled for a reasonable cost [11]. Four trends are detailed including increasingly destructive attacks, more targeted attacks against the manufacturing sector conducted by nation-states, adoption of contemporary technologies such as Artificial Intelligence by threat actors, and the continued improvements of efficiency in the cybercriminal environment to improve profitability.

Cybercrime is continuing to increase which is being powered by a cooperative clandestine supply structure that is evolving to be more professional and customized while supplying affordable and abundant tools and services [12]. Measurements of trust through a feedback and complaint notification methodology is being introduced in the world of cybercrime. The most prolific attack vector for malicious actors continues to be exploitation of unpatched vulnerabilities in widespread software [39]. An accelerating number and variety of cyber-attacks are occurring which is increasing the challenge in providing adequate security to protect confidential data. Ransomware-as-a-service offerings originating from and marketed by associations of threat actors have led to an excessive number of ransomware incidents [13]. The transformation of the business model regarding working from the office to working at home as a result of the COVID-19 lockdowns has resulted in growth of home Wi-Fi connectivity to business infrastructure and in turn, an increase cybercrime targeting personnel working from their home offices [14]. Several trends were outlined including the continued increase of COVID related threats, the proliferation of malware, the threats incurred with IoT technologies, the spread of ransomware related attacks, and the growing popularity of crypto jacking attacks.

Threats and mitigation techniques continue to develop in the sector of cybersecurity [15]. A list of trending cybersecurity topics were discussed including risks related to the remote working business methodology, cybercrime related to the continued proliferation and evolution of IoT related technologies, the increasing threat related to the continued proliferation of malware, threats related to the migration from organization owned data centers to cloud infrastructure, the continued improvement in effectiveness of social engineering related attacks, the growing exposure and number of compromises involving personally identifiable information (PII), the success of multi-factor authentication bypass techniques, concerns regarding cybercriminals making use of artificial intelligence in attack automation, and a variety of contemporary issues surrounding mobile security cybersecurity [15, 16]. Several contemporary cybersecurity trends that are continuing to evolve introducing risk to businesses, governments, and individuals in 2023 were discussed [16]. The proliferation of hybrid and remote work environments as well as smartphones were theorized as threats to personnel and companies. Several attack types including phishing, ransomware, crypto jacking, and other forms of social engineering were discussed as becoming more advanced while being spread more rapidly [36]. IoT devices and connected cars were recognized as increasing in risk and growing as a favorite target of hackers [37].

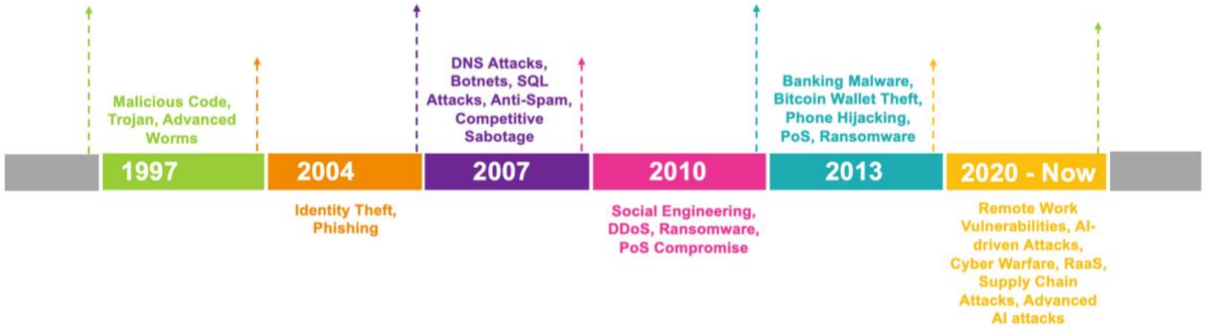

Figure 2: Evolution of Cybercrime Trends

Many trends agreed with other studies including the proliferation of ransomware, the usage of artificial intelligence in cyber-attacks, and the variety of criminal service offerings of crimeware-as-a-service. Satellite-based internet networks were discussed as a target of interest for cybercriminals to have a conduit to conduct Internet based attacks and to have another venue to blend malicious activity with normal traffic [17]. Money laundering-as-a-service with increased automation to reduce manual overhead as well as to provide concealment was also discussed. A concern was reasoned that threat actors are evolving to become more professional while creating business strategies to increase income streams [18]. Many of the same trends including the increasing threat of social engineering and ransomware, goring threats to the work at home business model, and security gaps with organizations migrating from company owned data centers to the cloud were debated [19]. Former techniques were recognized as being subjected to modification to bypass current security controls as one of the techniques used by cybercriminals to evolve. Many matching trends from other studies were mentioned including proliferation of phishing and other social engineering attacks, increased ransomware and malware incidents, the integration of AI and IoT devices into cybercrime, continued spread of crypto jacking, continued use of unpatched software as an initial attack vector [19]. Cyberactivism in which cybercrimes are committed for a political cause was recognized as a trending cybersecurity concern. An argument was made that encrypted communication applications such as Jaber and WhatsApp are being adopted by cybercriminals for communications to provide anonymity and increase difficulty in tracking down the threat actors [20].

3. METHODOLOGY

This systematic literature review strives to focus on the research problem of identifying contemporary threats and key trends in cybercrime at the present time. As significant effort has been undertaken and circulated in a variety of settings and by many organizations, a systematic literature review was conducted to research this problem. The research methods and questions utilized to reach the conclusions are discussed in the remainder of this section.

3.1 Analyzing the Emerging Trends in Cybercrime

The main research question that this analysis is centered around was “what are the current threats and trends that have been identified in recent research in the Dark Web and cybercrime?”. To identify appropriate resources, a few research questions were created.

- **RQ1:** What is the relationship between Dark Web and cybercrime?
- **RQ2:** Does the research provide insight into cybercrime activity that is accelerating in occurrence?
- **RQ3:** What has changed in the cybercrime ecosystem?
- **RQ4:** What benefits do these new trends provide cybercriminals?
- **RQ5:** Why are these cybercriminal activities trending?
- **RQ6:** What are the implications to the victims to the trending cybercrimes?
- **RQ7:** What date was the research work published?

Relying on the topics pertaining to the questions above, Google Scholar, IEEE Xplore, and UC’s Grover M. Hermann Library search utilities were used to locate scholarly journal entries and

articles. The same topics from the questions were used to search for well-known independent news articles and blog posts. While conducting the research of the sources identified during these searches, each individual source was evaluated based upon applicability to the selected topics regarding cybercrime, emerging trends, and publication time.

4. RESULTS

Cybercrime is undergoing a swift evolution which has developed into a well-structured ecosystem. Ransomware incidents have intensified substantially in recent years. Organizations that were subjected to attacks have almost doubled since 2021. The scale of transformation continues to accelerate with organizations financing many advancements in technology to increase efficiency and remain competitive [29]. Currently, IT systems are being enhanced for adopting remote work as part of the normal paradigm, augmenting consumer interfaces, and producing benefits which all give rise to threats and risks. For instance, during COVID-19, the workplace strategy shifted to enable work-at-home for nearly 50 percent of employees which heightened wireless internet connectivity usage within homes to attach to company networks which represents a reduced security connectivity model for employee communication.

Simultaneously, cybercriminals have organized into mature associations making use of a cohesive toolset with contemporary strategies including machine learning and artificial intelligence. Greater efficiency will be a goal of cybercriminals to enhance the return on investment of both time and resources [31]. As emerging technologies become mainstream, cybercriminals are learning how to weaponize these to facilitate an even greater amount of damage and interference. This can be seen in enhancements to cyber threats which are growing progressively ubiquitous through continued advancements and operational efficiencies which has in turn led to the commoditization of cybercrime as well as the introduction of a managed services pattern [30]. The amount and variability of cyber threats will sustain work for security personnel well into the future. Organizations of all sizes are currently confronted with the same threats with none being impervious. Management from all organizations must continually evaluate and improve their security controls and apply their current technology investments in a manner to mitigate threats over the next few years [32].

4.1 Threats & Trends

Presented below is a comprehensive list of identified threats and emerging trends. This catalog serves as a compilation illustrating the extensive analysis conducted to demonstrate the intrinsic research performed:

1. Novel technology usage by cybercriminals will continue to increase. For instance, criminals will adapt to using artificial intelligence as part of their attack regime. Cybercriminals are currently using AI to evolve their attacks such that they will be more successful. AI is currently being used for the credential deduction, bypassing CAPTCHA controls, as well as for the emulation of voices, and evading other security controls. This trend is expected to continue to evolve with significant advances in malicious innovations to intensify future cybercriminal activities. Some innovations are expected to include social engineering to trick users into navigating to malicious sites or revealing data that is

confidential. Another use of AI is through the development of videos called deepfakes which will superimpose a targeted individual's face in a video performing activities that they actually did not participate in [1]. Other cybercriminal activities that could be augmented by AI include writing technique impersonation, the deployment of chatbots to perplex victims, software development performed directly by AI, and the inclusion of AI directly into malware and ransomware to amplify results. AI and ransomware will increase vulnerabilities identified and locate victims while also assisting with detection evasion. It is expected that the scale of cyber-attacks will continue to increase because of the efficiencies that AI provides for cybercriminal operations [40].

2. As organizations have transformed into a business model that facilitates employees working from home on a more regular basis, trends in cybercrime are expected to continue to adapt to this model. The perimeter will be extended to include home networks as work equipment will continually relocate between different security zones represented by the home network and the secured network of the organization. Cybercriminals will attempt to take advantage of this with lateral movement between home networks and the organizations' networks [3]. One such cyber threat is related to phishing attacks that is centered around COVID-19 related topics. The cybercriminals act as if they are healthcare or governmental organizations to engage victims to respond regarding federal aid or healthcare related benefits using alarmist rhetoric.
3. Malware has become a mounting threat as it has transformed into a more efficient cybercriminal business model through the development of malware-as-a-service (MaaS). Enhanced malware is expected to lead to a large number of attacks targeting the theft of credentials as well as money and confidential data [4]. As more individuals work remotely, exposure is continued to increase for malware exploitation. Cybercriminals desire to target home networks as they are usually less secure than organizational infrastructure and have firewalls, routers, and other network devices that are not configured securely. Remote working distorts the boundaries of personal and work cultures which raises the possibility that confidential data could be compromised. This enables a larger number of cybercriminals to conduct operations using malware given that only a minute group of individuals possess the ability to create malware development capabilities.
4. Ransomware is also presenting as a rising threat and has grown to include over 120 distinct families as cybercriminals have grown more skilled in concealing malicious instructions inside of seemingly legitimate business applications. As with malware, targets have been created due to the new remote work paradigm created during the COVID-19 pandemic [6]. In turn, the number of attacks and amount of ransom has ballooned as a consequence. The trend is for ransomware to become increasingly advanced through distribution within the Dark Web as well as the deployment of ML and AI into the code. Ransomware has evolved to begin making use of malware referred to as "wiper" which is more devastating and advanced than previous strains. Payloads will be enhanced to enable data extortion as well as to be cloud aware and the addition of the wiper malware is a sign that these attacks will

likely be combined with other cybercrime tactics in the future. This represents a new pattern for coercing payment from the intended target.

5. Damaging data denial incidents will transform to be even more devastating and are expected to begin targeting time-sensitive information generated by real-time sensors such as those found in Internet-of-Things (IoT) devices.
6. Manufacturing and related industries will be the victims of more targeted attacks using Advanced Persistent Threats (APT) techniques conducted by nation states.
7. Another trend due to technological advancement is the proliferation of IoT into an attack surface that has greatly expanded. Given the increase in IoT devices, there has been a related 300 percent rise in the number of attacks on IoT endpoints from 2018 to 2019. It is more challenging to enable security controls for IoT devices such as antivirus and firewalls because they have lower storage capacity and less processing power [8]. Attacks on IoT devices can be used to steal data, perform DoS attacks, lock access to critical devices for direct monetary benefit, and inflict environmental or personal harm.
8. Another expanding trend is crypto jacking which is a specific malware attack type designed to compromise a computer and use the computer's resources to perform cryptocurrency mining. This attack method is considered by cybercriminals to be lower risk and easy to conduct resulting in a continuous flow of revenue. Crypto mining related malware has become highly available which is making this threat something that will continue to increase in popularity among cybercriminals [19]. There are a large number of possible targets with minimal effort for payout and any foothold achieved with cryptojacking could also potentially be used for exfiltrating data.
9. Another technological trend that continues to spread is the deployment of corporate resources using cloud services which have caused security concerns for institutions. Cloud environments have been implicated in a variety of exploits resulting in information leakage and unauthorized access, interfaces that have not been configured securely, and the hijacking of user accounts [10]. Security controls are expected to be inconsistently applied to cloud deployments since many security organizations do not have the experience or bandwidth to manage cloud environments. This will lead to misconfigurations as well as the delay of implemented security controls as the development of the cloud environment occurs.
10. Social engineering is expected to also adapt to the increased use of remote work culture as personnel working from home are less complicated victims. These social engineering attacks would include phishing, SMS phishing (smishing), and voice phishing (vishing). New phishing attacks are expected to adopt ML to streamline the creation and dissemination of persuasive fraudulent messages to trick victims into providing unauthorized access to their organization's infrastructure [12]. The number of smishing attacks are increasing because of the elevated use of mobile applications such as Skype, Teams, Zoom, WhatsApp, WeChat, and Signal. These applications are targeted to deceive users into the installation of malware onto their mobile devices [37]. With vishing,

employees are deceived by cybercriminals impersonating IT helpdesk employees and tricked into authorizing access to critical systems.

11. Another trend that is emerging is the increased concentration of malicious actors on techniques to bypass multi-factor authentication (MFA). Cybercriminals are concentrating on efforts to dissect MFA carried out through SMS and phone calls.
12. Recent developments in automobile-related technology have exposed them to direct exploitation allowing the theft of sensitive information, the actual theft of the automobile, and can directly instigate harm upon the drivers.
13. Many new concerns regarding mobile technology are being identified including spyware, vulnerability exploitation, and mobile malware. With spyware, cybercriminals can interact with applications responsible for encrypted messaging [14]. Mobile malware has introduced a number of security situations including data theft, spam over SMS, DDoS attacks using mobile devices, and compromising inadequate password security.
14. As satellite-based internet networks have become mainstream with additional size and dimension, they have also presented themselves as a new attack vector for cybercriminals. The largest targets for satellite-based attacks are organizations with low latency requirements delivered through the connectivity provided by satellite-based internet networks [17]. These organizations are within the transportation, shipping, and energy business sectors. Also, cybercriminals have targeted satellite communications in Ukraine due to the ongoing conflict. Cybercriminals seek to compromise these satellite networks to conceal their activities so that they can remain anonymous.
15. An increasing amount of new attack vectors are being enabled through the Dark Web as CaaS business offerings. As an extension to RaaS and other MaaS capabilities, the trend of new illicit services is expected to surge with a continued sale of the subscription-paid crime services in the future. The subscription-based offerings enable cybercriminals with rudimentary skills to launch advanced attacks with minimal investment of time and finances, and resources to develop a distinct tailored strategy [21]. This service offering enables experienced cybercriminals to sell attacks based on their skills quickly while providing a reliable income stream. As there is demand from unskilled cybercriminals and supply from experienced cybercriminals, the trend is expected to see CaaS continue to expand offerings in 2023 and the future. New emerging attack vectors are expected to be offered by cybercriminals such as deepfakes creation technology for sale [24]. Reconnaissance-as-a-service is expected to improve in demand with cybercriminals employing researchers to obtain intelligence on selected targets prior to executing an attack.
16. Another anticipated direction for the future of money laundering is that cybercriminals will make use of ML to improve the recruitment of money mules by identifying better targets as well as making the location of the mule recruits more efficient [12]. Operational improvements are expected to be made for manual mule campaigns to transform them into automated services to transport money through a variety of crypto markets to expedite the

movement procedure as well as to conceal the money transfer process while lowering the probability of fund recovery in the end [16]. Money Laundering-as-a-service is anticipated to be an integral part of the CaaS portfolio in the near future which will decrease the manual recruiting of mules and possibly remove it entirely.

17. The development of business email compromise (BEC) swindles will continue to flourish with progressively directed attacks. BEC selected as targets of cyber-attacks generally had relationships with overseas suppliers and performed online money transfers [19]. During these attacks, the cybercriminals will mimic the merchants or clients to compromise monetary transfers and send the money to attacker owned accounts.
18. As alluded to in some of the other predictions, cooperation and specialization are occurring in the world of cybercrime. Cybercrime has evolved to be performed by coordinated units of hackers. Specialization in different forms of cybercrime is also occurring including the publishing of viruses, the theft of confidential information, the performance of DDoS attacks, and the compromise of networks owned by organizations [26]. Collaboration and specialization enable the execution of extremely complex and destructive operations that an individual hacker may not be able to perform alone.
19. Cooperation between nation-state threat actors and cybercriminals is an expanding threat with broad repercussions. Nation states can offer cybercriminals a large number of resources and skills to execute advanced attacks, while cybercriminals seek monetary gain and are inclined to work for larger compensation [31]. Together, these considerations make it predictable that increasingly advanced cybercrime will occur.
20. Small-medium businesses (SMBs) are expected to become increasingly targeted due to the fact that they lack strong threat detection and prevention controls.
21. Cyberactivism is a trending type of cybercrime in which protesters are struggling for a specific political cause. One main focus is to interfere with the operations of an organization's website to send a message to management or to communicate knowledge regarding harmful activities performed by an organization.
22. Supply chains will continue to be targeted by cybercriminals through selected vulnerabilities concentrating on third-party provided components within an organization's environment.
23. The proliferation of encrypted communication by cybercriminals is continuing to increase. This is important for cybercriminals because encrypted communications retain anonymity and are challenging to track [22]. Law enforcement agencies are severely hampered by encrypted communications as this makes it extremely tricky to decrypt the communications with details of the criminal activities.
24. Cryptocurrency specifically Bitcoin has developed into the utmost prevalent ransom payout mechanism due to its anonymity, decentralization, and value.
25. Unpatched vulnerabilities remain a preferred path of compromise by cybercriminals who continuously search the internet for instances of these vulnerabilities. Upon discovery of

an instance of the vulnerability, the cybercriminals will exploit the vulnerability to compromise the system.

26. Remote Desktop Protocol (RDP) has evolved into a primary entry point for cybercriminals to obtain a foothold in an organization with targets with SMBs typically being targeted [23]. Credentials for RDP grant remote access into an organization's ecosystem which can be used to exfiltrate data or to lock access to critical systems.
27. 5G cellular has the capacity to relay information 300 percent quicker than 4G cellular along with the capability to integrate more individuals and computing equipment due to IoT technology. In turn, 5G has manifested into a target for cybercriminals to make their malicious operations more expedient and efficient.
28. As organizations integrate big data architecture into their operations, they have begun to gather large amounts of behavioral data regarding clients, vendors, and partners ranging from energy usage to financial information as well as usage of social networking platforms. With this expansion of data collection, cybercriminals continue to target and exploit big data infrastructure components.
29. The latest online applications make use of a number of contemporary technologies including virtual reality, augmented reality, and mixed reality which provide end users with an extremely innovative interface. These technologies have virtual resources associated with the accounts related to the users making them ongoing targets for cybercriminals and attacks targeting these resources are expected to rise [10].

The pie chart highlights the distribution of common cybercrime attack methods such as Social Engineering, Ransomware, Phishing, and IoT Vulnerabilities.

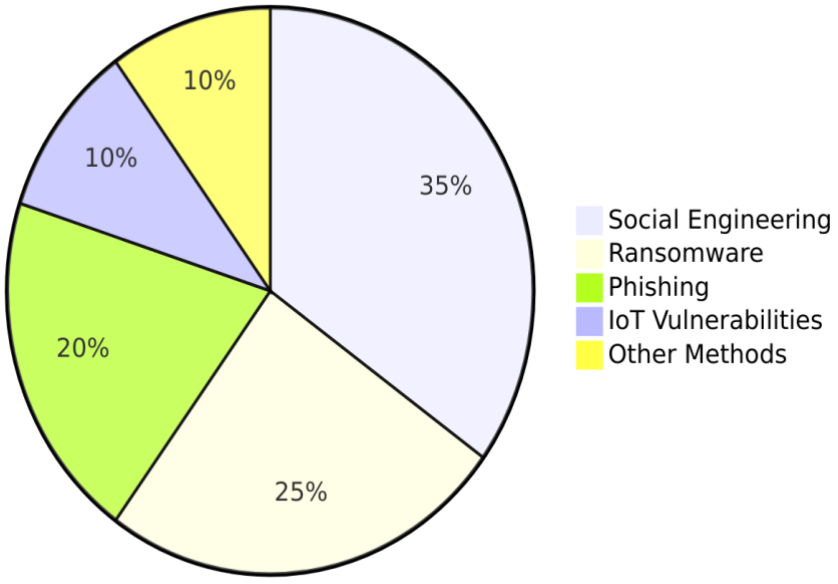

Figure 3: Common Cyber-attack Methods

5. DISCUSSION

Innovative progress has accelerated in the recent past including organizational shift into cloud environments and further individual adoption of mobile and contactless technologies. The digital ecosystem has continued to extend for companies as well as individuals which have expanded the attack surface for both exposing security gaps that have yet to be adequately addressed and thus left open for cybercriminals to exploit [14]. The capabilities and tactics used by cybercriminals have shifted to be increasingly more successful and proficient through the creation of new business strategies to offer hacking skills as commoditized services.

Understanding Cybercriminal Behavior

A criminological perspective provides valuable insights into the underlying mechanisms driving the growth and sophistication of cybercrime on the Dark Web. Routine Activity Theory (RAT) is relevant in explaining why cybercrime has proliferated in recent years. According to RAT, a crime occurs when three conditions converge: a motivated offender, a suitable target, and the absence of capable guardianship [41]. The anonymity of the Dark Web provides offenders with a high level of protection from detection and prosecution create an environment where motivated offenders can easily find suitable targets such as vulnerable systems, organizations with weak cybersecurity practices without immediate risks of being caught. The emergence of RaaS and CaaS commodified cybercrime making it easily accessible. This development is supported by Rational Choice Theory which posits that criminals weigh the potential rewards of their actions against the risks and costs [42]. The low risk of apprehension combined with the lucrative rewards of cybercrime such as large ransom payments makes this a rational choice for many individuals when sophisticated hacking tools can be purchased or leased with ease. Strain theory suggests that individuals turn to crime when they are unable to achieve socially accepted goals through legitimate means which further explains the rising engagement in cybercrime [43]. Economic disparities and limited employment opportunities in regions suffering from prolonged recessions or in post-pandemic recovery push individuals toward illegal cyber activities which offer an alternative means to achieve financial gain in a low-risk environment.

The Role of Economic Instability

The rise of cybercrime on the Dark Web cannot be fully understood without considering the socio-economic factors at play. The global economy has faced significant challenges in recent years including economic downturns, rising unemployment rates, and the destabilization brought about by the COVID-19 pandemic. Individuals with technological skills may turn to cybercrime as a form of income generation in times of economic uncertainty. Cybercrime offers a low-barrier entry into illicit activities when services like CaaS provide pre-packaged tools for launching attacks. This democratization of cybercrime parallels the broader economic shifts towards "gig economies" and "on-demand" services where individuals look for flexible, non-traditional income streams. The Dark Web provides a platform for income generation that appeals to those on the fringes of the economy as legitimate employment opportunities become more uncertain. Socio-political instability in certain regions has led to the emergence of cybercriminal groups with political or ideological motivations. For instance, hacktivist groups may exploit the Dark Web not

only for financial gain but also to promote political ideologies or challenge governmental control. These cyber actors often justify their actions as a form of protest or resistance against political and economic systems they perceive as oppressive.

The Impact of Anonymity and Deterrence

The anonymity afforded by the Dark Web plays a critical role in emboldening individuals to engage in illicit activities that they might not otherwise consider in a more transparent environment . De-individuation theory helps explain this behavior as it suggests that when individuals feel anonymous or part of a crowd, they experience a loss of self-awareness and are more likely to engage in behaviors that violate social norms [45]. The Dark Web with its layers of encryption and use of anonymizing tools like TOR fosters this de-individuation by allowing individuals to act with a reduced sense of accountability. Deterrence theory implies that individuals are less likely to commit crimes if they perceive the likelihood of being caught and punished to be high [44]. The perceived lack of deterrence plays a major role in motivating criminal behavior. Cybercriminals operating on the Dark Web often believe they are beyond the reach of law enforcement due to the complexities of tracking digital activities across borders. This perceived impunity creates an environment where even the most destructive forms of cybercrime such as ransomware attacks on critical infrastructure can be carried out with minimal fear of consequences. The lack of immediate punishment or visible harm may also distance cybercriminals from the consequences of their actions allowing them to rationalize their behavior. Unlike physical crimes where the damage is more tangible, cybercrimes often affect distant victims whom the perpetrator never sees reducing any sense of personal responsibility.

Challenges in Cyber Law

The rapid evolution of cybercrime is also a reflection of the inadequacies in the current legal and regulatory frameworks governing cyber activities. International law enforcement agencies face significant challenges in prosecuting cybercriminals operating on the Dark Web. The anonymity and decentralized nature of the Dark Web make it difficult for law enforcement to track and apprehend individuals who often operate in jurisdictions with weak or non-existent cybercrime laws [46]. This lack of robust international cooperation and harmonization of cyber laws creates a safe haven for cybercriminals. Nation-state actors can use the Dark Web to outsource attacks to leverage he skills and services of cybercriminal groups to engage in economic espionage, intellectual property theft, and even the disruption of critical infrastructure in rival countries [47]. These attacks are often politically motivated but are conducted in a way that offers plausible deniability for the state actors involved.

The development of more comprehensive and enforceable cyber laws is imperative as cybercrime intersects with national security [49]. The pace at which cyber laws are evolving lags behind the rapid innovation seen in cybercrime techniques. The commoditization of cybercrime services such as RaaS has transformed hacking from a niche skill into a service available to virtually anyone including individuals who may not fully understand the legal ramifications of their actions [48]. Governments and regulatory bodies need to catch up by creating clearer and more enforceable cybercrime laws that reflect the complexities of the modern digital landscape.

The European Union's General Data Protection Regulation (GDPR) and similar data protection frameworks offer some hope as they impose strict regulations on data handling and cyber responsibilities but these regulations mainly apply to legitimate organizations leaving the Dark Web largely unchecked [46].

6. CONCLUSION

Cybercrime is continuing to transform and accelerate along with technological advances that have occurred in recent times. The Dark Web has facilitated cybercrime's evolution by supplying an ecosystem that enables collaboration, sharing and distribution of ideas and tools, organization for planning criminal activities, training venues, and stores that trade in criminal merchandize, services, and information. There are multiple factors contributing to emerging trends in cybercrime. The main factor that continues to attribute to the acceleration of cybercrime is unpatched software and infrastructure components which are commonly used as an anchorage for cybercriminals to obtain unauthorized access into the organizational networks. Another critical factor is the commoditization of services to facilitate cybercrime which allows individuals with novice skillset to continue sophisticated cybercrime activities while at the same time producing a revenue stream for accomplished cybercriminals with in-demand skills. Also, contemporary technologies such as artificial intelligence and machine learning, satellite communication networks, IoT devices, automobiles with computing interfaces, 5G network rollout, migration from corporate data centers to cloud environments, the proliferation of big data technologies provide new avenues with security issues that cybercriminals can exploit. Another factor that has led to the acceleration of cybercrime is the migration of employees to remote working model which has elevated the attack surface for organizations.

7. DIRECTIONS OF FUTURE STUDY

Cybercrime is expected to further accelerate as novel technologies emerge. Quantum computing while still in its infancy is expected to lead to drastically improved computing environment in the future. When this occurs, the computing power could render many existing encryption methodologies obsolete overnight leading to the compromise of confidential information that is otherwise protected in today's computing environment. In the future, virtual goods in augmented reality and virtual reality settings are expected to become targets of cybercrime activities. As AI applications continue to proliferate and evolve, cybercriminals will make use of these applications to develop more efficient and illicit lucrative schemes. Lastly, deepfake technology is expected to become extremely realistic with cybercriminals currently planning scenarios to trick individuals into interacting with familiar voices and faces to extort money and information.

References

[1] Zhang, H., & Zou, F. (2020). A Survey of the Dark Web and Dark Market Research. *In 2020 IEEE 6th International Conference on Computer and Communications (ICCC)*. https://doi.org/10.1109/iccc51575.2020.9345271.

[2] Schäfer, M., Fuchs, M., Strohmeier, M., Engel, M., Liechti, M., & Lenders, V. (2019). BlackWidow: Monitoring the Dark Web for Cyber Security Information. *2019 11th*

International Conference on Cyber Conflict (CyCon), 1-21. https://doi.org/10.23919/CYCON.2019.8756845

[3] Cascavilla, G., Tamburri, D. A., & Van Den Heuvel W. J. (2021). Cybercrime threat intelligence: A systematic multi-vocal literature review. *Computers & Security*, *105*. doi: https://doi.org/10.1016/j.cose.2021.102258.

[4] Adewopo, V., Gonen, B., & Adewopo, F. (2020). Exploring Open Source Information for Cyber Threat Intelligence. *In 2020 IEEE International Conference on Big Data (Big Data)*. https://doi.org/10.1109/BigData50022.2020.9378220.

[5] Samtani, S., Zhu, H., & Chen, H. (2020). Proactively Identifying Emerging Hacker Threats from the Dark Web: A Diachronic Graph Embedding Framework (D-GEF). *ACM Transactions on Privacy and Security*, *23*(4), 1–33. https://doi.org/10.1145/3409289.

[6] Holt, T. J. (2012). Examining the Forces Shaping Cybercrime Markets Online. *Social Science Computer Review*, *31*(2), 165–177. https://doi.org/10.1177/0894439312452998.

[7] Rawat, R., Ajagbe, S. A., & Oki O. A. (2022). Techniques for Predicting Dark Web Events Focused on the Delivery of Illicit Products and Ordered Crime. https://doi.org/10.21203/rs.3.rs-1665267/v1.

[8] Rudesill, D. S., Caverlee, J., & Sui, D. (2015). The Deep Web and the Darknet: A Look Inside the Internet's Massive Black Box. *SSRN Electronic Journal*. https://doi.org/10.2139/ssrn.2676615.

[9] Basheer, R. & Alkhatib, B (2021). Threats from the Dark: A Review over Dark Web Investigation Research for Cyber Threat Intelligence. *Journal of Computer Networks and Communications*, *2021*, https://doi.org/10.1155/2021/1302999.

[10] Świątkowska, J. (2020). Tackling cybercrime to unleash developing countries' digital potential. https://pathwayscommission.bsg.ox.ac.uk/sites/default/files/2020-01/tackling_cybercrime_to_unleash_developing_countries_digital_potential.pdf/

[11] Townsend, K. (2022). Understanding the Evolution of Cybercrime to Predict its Future. *SecurityWeek*, https://www.securityweek.com/understanding-evolution-cybercrime-predict-its-future/

[12] Security, H. W. (2022). The Evolution of Cybercrime: Why the Dark Web is Supercharging the Threat Landscape and How to Fight Back. *HP Wolf Security*, https://threatresearch.ext.hp.com/evolution-of-cybercrime-report/

[13] Enterprise, B. (2022). What Are The Biggest Cyber Threats of The Future? *BitDefender*. https://businessinsights.bitdefender.com/what-are-the-biggest-cyber-threats-of-the-future/

[14] Kelly, P. (2023). Trends in Cybercrime in 2022 and Beyond. https://blog.govnet.co.uk/technology/trends-in-cybercrime-in-and-beyond/

[15] Kaspersky. (2019). 4 Cyber Security Trends to Keep an Eye On. https://www.kaspersky.com/resource-center/preemptive-safety/cyber-security-trends/

[16] Top Cybersecurity Threats. (2023). University of San Diego Online Degrees. https://onlinedegrees.sandiego.edu/top-cyber-security-threats/#threats-and-trends/

[17] Fortinet. (2022). Cyber Threat Predictions for 2023 An Annual Perspective by FortiGuard Labs. https://www.fortinet.com/content/dam/maindam/PUBLIC/02_MARKETING/02_Collateral/WhitePaper/WP-threat-prediction-2023.pdf/

[18] Micro, T. (2022). Future/Tense: Trend Micro Security Predictions 2023 - Security Predictions. https://www.trendmicro.com/vinfo/us/security/research-and-analysis/predictions/2023/

[19] Eira, A. (2019). 16 Latest Cybercrime Trends & Predictions for 2021/2022 and Beyond. *Financesonline.com*. https://financesonline.com/cybercrime-trends/

[20] Sindelar, E. & Ferguson, R. (2021). Cybercrime: Today and the Future. *Trend Micro*, https://www.trendmicro.com/en_us/ciso/21/h/cybercrime-today-and-the-future.html/

[21] Weigand, S. (2023). 2023 threat predictions: Beware 'economic uncertainty' for the cybersecurity community. *SC Media*. https://www.scmagazine.com/feature/third-party-risk/2023-threat-predictions-beware-economic-uncertainty-for-the-cybersecurity-community/

[22] Carmiel, D. (2022). Council Post: 5 Trends Shaping The Future Of Cybercrime Threat Intelligence. *Forbes*. https://www.forbes.com/sites/forbestechcouncil/2022/12/19/5-trends-shaping-the-future-of-cybercrime-threat-intelligence/

[23] Glas, K. (2021). What Will the Future of Cybercrime Look Like? *TFOT*. https://thefutureofthings.com/15904-what-will-the-future-of-cybercrime-look-like/

[24] Boehm, J., Lewis, C., Li, K., Wallance, D., & Dias, D. (2022). Cybersecurity trends: Looking over the horizon. *McKinsey*, https://www.mckinsey.com/capabilities/risk-and-resilience/our-insights/cybersecurity/cybersecurity-trends-looking-over-the-horizon/

[25] Ryan, P. (2023). How the future of cyber crime could involve fake voice messages from loved ones? *The National News*. https://www.thenationalnews.com/uae/2023/03/17/how-the-future-of-cybercrime-could-involve-fake-voice-messages-from-loved-ones/

[26] Morgan, S. (2020). Global Cybercrime Damages Predicted To Reach $6 Trillion Annually By 2021. *Cybercrime Magazine*. https://cybersecurityventures.com/cybercrime-damages-6-trillion-by-2021/

[27] Labs, F. (2022). Threat Predictions for 2023: New Attack Surfaces and Threats Emerge as Cybercrime Expands. *Fortinet Blog*. https://www.fortinet.com/blog/threat-research/2023-threat-predictions-new-attack-surfaces-threats-emerge-cybercrime-expands/

[28] Mador, Z. (2022). Infiltrating the Dark Web for Threat Intelligence Collaboration. *CPO Magazine*. https://www.cpomagazine.com/cyber-security/infiltrating-the-dark-web-for-threat-intelligence-collaboration/

[29] Bowers, K. (2018). Dark Web Chatter Helpful in Predicting Real World Hacks, Firm Says. *SecurityWeek*. https://www.securityweek.com/dark-web-chatter-helpful-predicting-real-world-hacks-firm-says/

[30] Paganini, P. (2020). The Crimeware-as-a-Service model is sweeping over the cybercrime world. Here's why. *CyberNews*. https://cybernews.com/security/crimeware-as-a-service-model-is-sweeping-over-the-cybercrime-world/

[31] Cerulus, L. (2021). One group that's embraced AI: Criminals. *POLITICO*. https://www.politico.eu/article/artificial-intelligence-criminals/

[32] Consulting, P., A. (2023). Why the 'dark web' is becoming a cyber security nightmare for businesses. *PA Consulting*. https://www.paconsulting.com/insights/why-the-dark-web-is-becoming-a-cyber-security-nightmare-for-businesses/.

[33] Singh, T. (2024). Dark Web Dynamics: Investigating Cybercrime Trends And Regulatory Responses In The Digital Age. *Revista Electronica de Veterinaria*, *25*(1S), 612-618. https://doi.org/10.69980/redvet.v25i1S.791

[34] Montasari, R., & Hopcraft, B. (2024). Securing Cyberspace: Addressing the Dark Web and Cybercrime Underreporting. In *Space Law Principles and Sustainable Measures*, 185-198. Cham: Springer Nature Switzerland. https://doi.org/10.1007/978-3-031-64045-2_9

[35] Kaur, G., Mukherjee, D., Moza, B., Pahwa, V., Kaur, K., & Kaur, K. (2024). The dark web: A hidden menace or a tool for privacy protection. *IP International Journal of Forensic Medicine and Toxicological Sciences*, *8*(4), 160-167. https://doi.org/10.18231/j.ijfmts.2023.034

[36] Sahu, S., Verma, P., & Kashyap, P. (2023). Surveying the Dark Web: An overview of its Structure, Content, and Challenges. *International Journal of Gender, Science and Technology*, *12*(2), 46-54. https://ijgst.com/admin/uploadss/Paper8-IJGST-DECEMBER-2023.pdf

[37] Anzaruddin, M., Shoaib, S. I., Dangwal, I., Nand, P., Agarwal, I., & Astya, R. (2024). The Enigma of the Dark Web: A Duality of Unrestricted Liberty and Unlawfulness. *In 2024 Sixth International Conference on Computational Intelligence and Communication Technologies (CCICT)*, *IEEE*, 273-278. https://doi.org/10.1109/CCICT62777.2024.00053.

[38] Biedron, S. R. (2024). *Cybercrime in the Digital Age* (Doctoral dissertation, University of Oxford).

[39] Malik, S., Rana, A., & Chauhan, M. (2024). The Dark Web: An Analysis of its Structure, Activities and Implications. *Journal of Network & Information Security*, *12*(1), 39-46.

[40] Holmes, L. (2024). Cybercrime. In *Rethinking Organised Crime*. Edward Elgar Publishing, 26-42. https://doi.org/10.4337/9781802206234.00007

[41] Özaşçılar, M., Çalıcı, C., & Vakhitova, Z. (2024). Examining cybercrime victimisation among Turkish women using routine activity theory. *Crime Prevention and Community Safety*, *26*(1), 112-128.

[42] Steinmetz, K. F., & Pratt, T. C. (2024). Revisiting the tautology problem in rational choice theory: What it is and how to move forward theoretically and empirically. *European Journal of Criminology*.

[43] Meehan, T., Forrester, L., & Haaja, J. A. (2024). Sociological Theories of Crime: Strain Theories. *Introduction to Criminology and Criminal Justice*, Open Educational Resources Collective.

[44] Kłusek, M. (2024). How acceptable is optimal deterrence?. *International Review of Law and Economics*, *78*, 106194.

[45] Martin Coesel, A., Biancardi, B., & Buisine, S. (2024). A theoretical review of the Proteus effect: understanding the underlying processes. *Frontiers in Psychology*, *15*, 1379599.

[46] Ruddin, I., & SGN, S. Z. (2024). Evolution of Cybercrime Law in Legal Development in the Digital World. *Jurnal Multidisiplin Madani*, *4*(1), 168-173.

[47] Li, Z. (2024). The Evolution of Internet Law in The Digital Age. *International Journal of Education and Humanities*, *13*(2), 124-126.

[48] Buçaj, E., & Idrizaj, K. (2025). The need for cybercrime regulation on a global scale by the international law and cyber convention. *Multidisciplinary Reviews*, *8*(1), 2025024-2025024.

[49] Joshi, A. (2024). Study of Cybersecurity Laws and Regulations. *Indian Journal of Law*, *2*(3), 7-14.

ACKNOWLEDGEMENTS

My mentor's constant support and guidance facilitated the achievement of excellence in my research. Chris provided constructive criticism, expert insights, and ideas that enabled me to improve my arguments and explore my research questions with more depth. Without his help, I would not have been able to achieve the level of quality I aimed for.

Conflict of Interest

I declare no competing interests.

Availability of data and materials

Data sharing is not applicable to this article as no datasets were generated or analyzed during the current study.

Funding

This research received no specific grant from any funding agency in the public, commercial, or not-for-profit sectors.

Authors' Contributions

ST designed the study, conducted the research, collected and analyzed the data, and wrote the manuscript. ST read and approved the final manuscript.

Authors' information

ST is currently employed as a research scientist at a leading financial institution in the United States where I specialize in the field of cybersecurity. Besides working as a research scientist, ST pursuing a Ph.D. in Information Technology with a concentration in Information Systems Security. ST also holds a distinguished Master's degree in Computer Science with honors conferred by Oklahoma City University (OKCU).