Scientific Research Publishing

Open Journal of Business and Management, 2024, 12, 293-338
https://www.scirp.org/journal/ojbm
ISSN Online: 2329-3292
ISSN Print: 2329-3284

The Evolution of Integrated Advance Persistent Threat and Its Defense Solutions: A Literature Review

Jun Zhang, Dan Tenney

Technology Management Department, School of Engineering, University of Bridgeport, Bridgeport, USA
Email: zhangjun@bridgeport.edu

How to cite this paper: Zhang, J., & Tenney, D. (2024). The Evolution of Integrated Advance Persistent Threat and Its Defense Solutions: A Literature Review. *Open Journal of Business and Management, 12,* 293-338.
https://doi.org/10.4236/ojbm.2024.121021

Received: October 21, 2023
Accepted: January 23, 2024
Published: January 26, 2024

Abstract

In 2023, the dawn of Generative Artificial Intelligence, cybercriminals thrive in the underground domain of the dark web ecosystem, powered by cutting-edge technology and all sorts of Cybercrime-as-a-Service weaponry. This complete dark supply chain offers a diverse array of vicious yet non-tech savvy friendly services, from Phishing to Malware. This can significantly lower the barriers to entry for even non-tech savvy person to launch IAPT attacks against large targets such as governments and corporations, as social engineering is the only required skill which now can be augmented by Large Language Models. Despite this gruesome reality, the current academic research lacks a comprehensive understanding such arsenal of Integrated Advanced Persistent Threats (IAPT) within the dark web ecosystem. This work aims to bridge the knowledge gap with a comprehensive literature review on IAPT, which is nowadays augmented with threat infrastructure. It will analyze the attack chain, highlight notable CaaS providers and techniques, and discuss possible defense strategies with the consideration of small to medium-sized enterprises (SMEs). It will also motivate further research in the new area of Psybersecurity/Secoanalysis by incorporating psychological/psychoanalytical, sociocultural, and sociopolitical tools into cybersecurity and management.

Keywords

Generative Artificial Intelligence, Cybersecurity Management, Cybercrime Analysis, Social Engineering, Advanced Persistent Threats

1. Introduction

In 2023, Microsoft released its Digital Defense Report (Microsoft Digital Defense

Report 2023 (MDDR)|Microsoft Security Insider, n.d.), providing valuable insights into the current cybersecurity landscape. Over the past four years, attacks on open-source software have surged by a staggering 742%. Alarmingly, less than 15% of non-governmental organizations (NGOs) employ cybersecurity experts. A concerning trend emerged, with 4.2% of incident response cases revealing coin-mining activity. Additionally, 17% of intrusions exploited known remote monitoring and management tools, such as remote desktop protocol.

A noteworthy development is the rise of "Adversary in the Middle" (AITM) attacks, formerly known as "Man in the Middle" (MITM). These attacks involve phishing domains, which ballooned from 2000 active domains in June of the previous year to more than 9000 by April of the current year (Security Now! Transcript of Episode #943, n.d.). Phishing remains a prevalent method employed by malicious actors, providing them with unauthorized access. Businesses faced a significant threat from daily email compromise attempts, averaging 156,000 between April 2022 and April 2023. Critical infrastructure organizations, responsible for vital services like power generation and hydroelectric dams, bore the brunt of these attacks, receiving 41% of threat notifications (Microsoft Digital Defense Report 2023 (MDDR)|Microsoft Security Insider, n.d.; Security Now! Transcript of Episode #943, n.d.).

The shift to cloud services brought forth a surge in password-based attacks, prompting Microsoft to thwart an average of 4000 such attacks per second over the past year. Even multifactor authentication, a commonly relied upon security measure, faced assaults, with approximately 6000 fatigue attempts daily. Token replay attacks doubled in frequency, with an average of 11 detections per 100,000 active users in Azure Active Directory Identity Protection. Distributed Denial of Service (DDoS) attacks also surged, reaching 1700 attacks daily, generating an overwhelming 90 terabits of data per second (Microsoft Digital Defense Report 2023 (MDDR)|Microsoft Security Insider, n.d.). This scale of attack incapacitates online services, causing significant disruptions.

Regrettably, the cybersecurity landscape has witnessed explosive growth in cybercrime activity and intrusion attempts over the past year. This escalation is a cause for concern across the industry. Unlike other sectors, cybersecurity is experiencing unprecedented growth, highlighting the urgent need for enhanced digital defense strategies to safeguard businesses and critical infrastructure from these ever-evolving threats (Security Now! Transcript of Episode #924, n.d.).

The dark web market generated $2.1 billion in cryptocurrency revenue in 2021, with a significant portion coming from fraud shops. Stolen credit card data is available for as little as $25, and over 543 million assets tied to Fortune 1000 employees are on the dark web. The FBI's takedown of the Silk Road 2.0 site revealed sales of over $9.5 million in Bitcoin. India had the highest access to the dark web, and 90% of posts on dark web forums were from buyers looking to contact a criminal. A third of North Americans use the dark web regularly, and the number of dark web listings that could harm an enterprise is increasing. 45%

of bitcoin sent to the darknet comes from a KYC-free exchange (Soocial, 2022).

We have been studying ransomware from the WannaCry outbreak in 2017 to the rebranding of the threat actor groups such as DarkSide and REvil. Ransomware-as-a-Service (RaaS) is a new business model that follows Software-as-a-Service. RaaS is gaining popularity among cybercriminals due to reduced infrastructure costs, deployment times, and specialized social-engineering teams. This model allows criminals with limited technical knowledge to "rent" sophisticated ransomware (Keijzer, 2020). For example, in 2022, a new Phishing-as-a-Service (PhaaS) system advertised on the Dark Web, EvilProxy, which presents a significant threat to enterprises and organizations that rely on MFA for cybersecurity. Nevertheless, the success of the RaaS business model has now been followed by the emergence of all kinds of Cybercrime-as-a-Services (CaaSs)—such as Phishing-as-a-Service (PhaaS), Voice-Cloning-as-a-Service (VCaaS), Deepfakes-as-a-Service (DFaaS), Malware-as-a-Service (MaaS), and DDoS-as-a-Service (DDoSaaS), completing a diverse dark supply chain as cybercriminals' arsenal/infrastructure.

Numerous incident reports and research studies were published to either address a single threat or providing relative comprehensive yet outdated information. Therefore, no study exists in the literature that gives the complete yet up-to-date picture of Integrated Advanced Persistent Threats (IAPT) a new concept stemming from traditional Advanced Persistent Threats. Integrated Advanced Persistent Threats consist of six consecutive stages of attack, forming a chain of attacks. The APT attack nowadays can be augmented with open-source intelligence (OSINT), generative artificial intelligence and harvest cryptocurrency with ransomware attack.

There are numerous novel CaaS groups providing a variety of user-friendly attack toolkits, which have drawn significant attention within the security industry but have not yet been widely studied in academia timely. In this model, various specialized criminal services have emerged, such as Phishing-as-a-Service, which focuses on tricking individuals through social engineering, and Ransomware-as-a-Service, which focuses on extorting sensitive data. These services have significantly lowered the barriers for non-experts to launch damaging attacks against large targets like governments and organizations. As a result, social engineering is the only required (non-technical) skill which now can be augmented by Large Language Models (LLMs), an AI tool can be used to assist phishing campaign. When integrated with all tools of the dark supply-chain, threat actors can do significant damage by maliciously encrypting and exfiltrating confidential data in exchange for cryptocurrency.

The emergence of these threats has drawn significant attention in the security industry but has not yet been widely studied in academia. Moreover, most existing studies focus on individual aspects rather than providing a comprehensive analysis. Consequently, there are gaps in our understanding of the full scope of interactions among these components of Integrated Advanced Persistent Threats.

To address these gaps, and motivate further research, this paper presents a comprehensive literature review on IAPT with all kinds of CaaSs of the dark net and introduces a framework to visualize this concept.

This study gives a detailed overview of components of IAPT, comprehensively analyzes the possible attack chain of a typical ransomware operator, presents topology of notable CaaS providers, and provide an extensive overview of IAPT defense. This study aims to raise awareness of IAPT and discusses possible solutions for security researchers, professionals, and decision-makers in organizations. Because smaller businesses are at even higher risk due to their limited resources. It specifically considers the needs of small to medium sized enterprises (SMEs), which often have limited technical resources to defend against cybersecurity threats.

Despite these efforts, this study suggests that future research should adopt multidisciplinary approaches, integrating various research methods and theoretical perspectives. This study advocates for further research in the multidisciplinary approach of Psybersecurity and Secoanalysis, which combines social science tools to manage technology-related security issues. These new concepts aim to address the vulnerabilities of both individuals and society. By prioritizing education, training, policy changes, technological advancements, promoting an open culture, and incorporating psychoanalytic insights to counter social engineering threats, organizations can create safer work environments. Additionally, these measures promote democracy, equity, and transparency, benefiting all parties involved. This study asserts that this is crucial to tackle the enduring challenges posed by cybercrime. This study will motivate further research by presenting a complete picture on state-of-the-art Integrated Advanced Persistent Threat research in the era of Generative AI (Resecurity, 2022).

1.1. Statistics of Literature Survey (Table 1)

In the total of 80 reviewed literatures, Small and Medium-sized Enterprises (SMEs) find themselves particularly vulnerable, lacking adequate resources and research effort to effectively combat these threats as shown in **Figure 1**. Moreover, a notable gap in existing research on the area of Malicious AI Generated Content (MAIGC) for phishing attacks. Unlike traditional phishing attempts, MAIGC leverages Artificial Intelligence to create highly convincing deceptive content, making it increasingly difficult for victims to discern authentic communication from malicious intent. The proliferation of such malicious content has far-reaching consequences, by assisting social engineering stage of IAPT attack chain, especially for SMEs, as they often lack the complete, yet costly defense systems employed by larger enterprises.

While a substantial volume of literature addresses IAPT and related subcategories, **Figure 2** shows a significant number of literatures providing less detail. Also, SMEs are underrepresented in this body of work, despite constituting a critical segment of the business landscape. Notably, the proliferation of MAIGC,

Table 1. Statistics of literature survey.

Subcategories of IAPT	Statistics of Literature Survey		
	Hits of literature topics without details	Hits of literature topics with in-depth details	Hits of literature topics in total
OSINT	7	1	8
EvilProxy/AiTM	3	8	11
General MFA Bypassing	4	6	10
Water Hole/Spear-Phishing	4	3	7
General Social Engineering	14	10	24
MAIGC Phishing	11	9	20
Code/Script Generating	8	4	12
DFaaS/VCaaS	2	4	6
Other Dark AI	4	6	10
Encryption/Locker	11	16	27
Exfiltration	11	7	18
Ransom DDoS/Extortion	1	0	1
Other CaaS	1	2	3
DWM	10	17	27
Cryptocurrency	2	11	13
SMEs/SMBs Defense	2	1	3
Other Defense	10	21	31
Total	105	126	231

particularly within phishing reports, poses an imminent threat to the security of SMEs. Hence, understanding the scarcity of research in this context is of paramount significance. The increasingly abusive use of MAIGC in phishing attacks necessitates swift and well-informed action to curtail the potential ramifications for these smaller enterprises. This study underscores the critical need to address this emerging problem promptly to mitigate the damage it may inflict and protect the interests of SMEs in an interconnected digital ecosystem.

1.2. Main Contributions of the Research

This study alerts the danger of the new threat and discusses possible solutions for security researchers, professionals, and decision-makers of organizations.

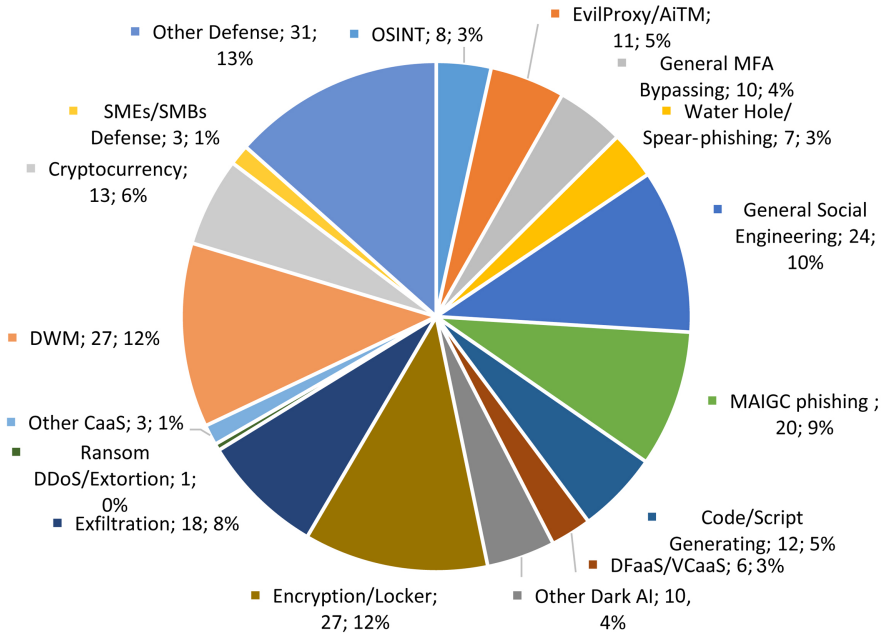

Figure 1. Distribution of literature topic hits by services/techniques.

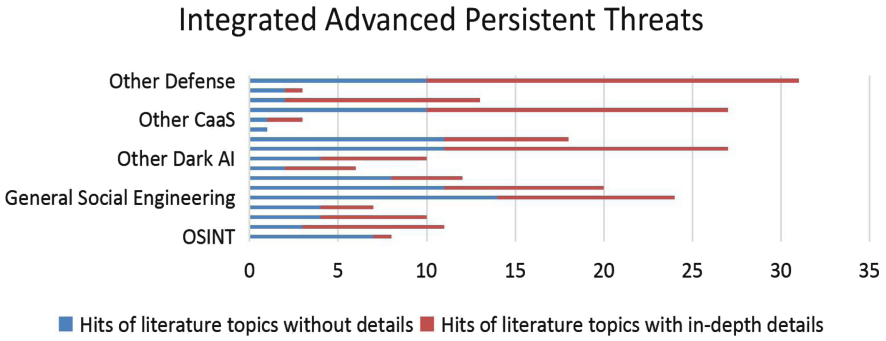

Figure 2. Hits of literature topics by details and subcategories.

Many of the alerts are originally spread from a reputable security researcher Steve Gibson in his podcast (Security Now! Transcript of Episode #924, n.d.; Security Now! Transcript of Episode #943, n.d.).

The study aimed to understand the IAPT interactions among its components, pathology of technopsychosocial factors, and potential treatment/solution. By proposing novel multidisciplinary approaches such as Psybersecurity and Secoanalysis are crucial in countering the evolving cybercrime such as IAPT.

2. Literature Survey

2.1. Phishing-as-a-Service

The rise of Phishing-as-a-Service (PhaaS) is a major concern for cybersecurity professionals and organizations. One notable PhaaS offering, EvilProxy, operates on its Telegram channel #EvilProxy [OFFICIAL CHANNEL] (evil_proxy, 2022) since May 11, 2022. EvilProxy provides guides, demo videos, and promotes itself

as a tool for carrying out phishing attacks on various online services. The channel also shares links to forums like XSS.is, breached.to, and forum.exploit.in, and has added Instagram as a new target. This underscores the growing trend of PhaaS, enabling non-technical individuals to conduct advanced phishing campaigns. Researchers and practitioners must study this threat and develop effective countermeasures to protect organizations and individuals. On July 4, 2022, a user advertised a "Phishing as a Service" (PhaaS) offering on a hacker forum (evilproxy, 2022). They claim it enhances resilience against phishing attacks and provides a range of functionalities for phishing campaigns. The services cover popular websites like Google, Microsoft, iCloud, and more, with different durations and prices. The post also mentions features like bot protection, virtualization detection, and automation detection. On September 5, 2022, Resecurity, a security research group, unveiled their findings on EvilProxy, a newly surfaced Phishing-as-a-Service system advertised on the Dark Web. EvilProxy facilitates the easy bypassing of Multi-Factor Authentication (MFA) through reverse proxy and cookie injection methods, posing a substantial threat to organizations relying on MFA for cybersecurity. While this PhaaS group, EvilProxy, has garnered significant attention in the security industry, it remains relatively unexplored in academic circles. The use of services like EvilProxy to outsource development processes can dramatically lower entry barriers for individuals or groups with limited technical expertise, enabling them to launch Advanced Persistent Threats (APTs) against high-value targets like governments and corporations, with only social engineering skills required (Resecurity, 2022). In Security Now! podcast episode #888 (Gibson & Laporte, n.d.), cybersecurity expert Steve Gibson discusses the emergence of EvilProxy, a new Phishing-as-a-Service system on the dark web. EvilProxy can bypass SMS, OAuth, and TOTP multi-factor authentication by intercepting authentication flows, posing a significant threat to online security. This turnkey service, discovered by Resecurity in May 2022, exploits web weaknesses by streaming websites through a transparent reverse proxy. EvilProxy's user-friendly interface makes it a potent threat, enabling non-technical individuals to launch advanced phishing campaigns easily. This research focuses on the threat of EvilProxy, particularly in the context of Ransomware-as-a-Service (RaaS) and its impact on organizations. The University of North Carolina's Information Security Office has issued a report (Trumbull, 2022) on methods used by malicious actors to evade strong security measures, particularly focusing on Multifactor Authentication (MFA) and MFA bypass techniques. While MFA enhances security by requiring multiple forms of authentication, attackers are determined to find ways around it. The report outlines common MFA bypass methods, including phishing emails or text messages leading users to fake sign-in pages. More advanced techniques like proxy attacks are also discussed, emphasizing the need for awareness, and understanding to enhance protection. The Microsoft 365 Defender Research Team and Microsoft Threat Intelligence Center (MSTIC) have reported a large-scale phishing campaign

using "adversary-in-the-middle" (AiTM) phishing. This technique aimed to steal passwords, hijack user sessions, and bypass multifactor authentication (MFA), even when enabled. Attackers used stolen credentials and session cookies for follow-on business email compromise (BEC) campaigns. This attack is similar to conventional phishing but exploits MFA vulnerabilities. To defend against such threats, the article recommends a comprehensive strategy, including conditional access policies and assuming a breach for improved network and threat data understanding (MSTIC, 2022). Evilproxy allows the attacker to set up a phishing site that proxies the legitimate website and can be used to facilitate AiTM phishing attacks. It is specifically designed to work in an adversary-in-the-middle (AiTM) phishing attack, which is a type of phishing attack where the attacker deploys a proxy server between the target user and the website they are trying to visit.

Cybercriminals are exploiting the death of Queen Elizabeth II in phishing attacks to steal Microsoft account credentials, according to a report (Gatlan, 2022) by Bleeping Computer on September 14, 2022. Attackers impersonate "the Microsoft team" and direct victims to a memorial technology hub, where they're prompted to enter their credentials on a phishing page. They're also trying to capture multi-factor authentication codes. The campaign uses a new reverse-proxy Phishing-as-a-Service (PaaS) platform called EvilProxy, enabling less-skilled actors to bypass MFA. The UK's National Cyber Security Centre warns of increased risks related to cybercriminals using the Queen's death in various scams and phishing campaigns. The Robin Banks Phishing-as-a-Service platform has recently targeted financial institutions in the U.S., U.K., Canada, and Australia, per IronNet research. Major banks like Bank of America, Wells Fargo, Capital One, and Citigroup have been under attack since March 2022. This platform offers ready-made phishing kits with a personal dashboard for wallet management and page creation. It also supports reCAPTCHA and user agent string checks. While the main goal seems to be financial, scammers using this kit also request victims' Google and Microsoft credentials, suggesting potential use by advanced threat actors seeking initial access to corporate networks for ransomware or other activities (Hoffman, 2022). This research (Khursheed et al., 2020) explores the link between microtargeting in digital marketing and phishing attacks. It proposes that methods used to gauge digital marketing campaign effectiveness can also aid in identifying and preventing phishing attacks. The study compares PhaaS (Phishing as a Service) to microtargeting, highlighting their data-focused approaches. It demonstrates that digital marketing metrics can enhance phishing analysis, revealing unexpected connections in phishing emails and the potential use of Microphishing for information gathering and analysis.

2.2. MFA Bypassing

Multi-factor authentication (MFA) requires multiple authentication methods for account access, increasing security. Attackers have sought to bypass MFA

using tools like EvilProxy and AiTM. Bezerra et al. conducted a systematic literature review titled "Characteristics and Main Threats about Multi-Factor Authentication: A Survey" to analyze the state-of-the-art in threat models and MFA. They selected 9 articles from 32 in the SCOPUS database and identified key characteristics and threats in the research area. The authors categorized articles into five areas: lightweight authentication, threat model methodology, authentication factors, MFA for Banks, and formal analyses. They identified 23 distinct threats across the articles (Bezerra et al., 2022). In "Hacking Multifactor Authentication" by Roger Grimes (Grimes, 2021), the author provides a comprehensive analysis of hacking methods for multifactor authentication (MFA) systems. The book covers various MFA types, such as hardware, software, and biometrics, detailing how each can be compromised. Grimes discusses specific hacking techniques for each type, like shoulder surfing and SIM swapping. He distinguishes MFA systems as either weak or strong, advocating for stronger options like phone apps with push notifications, FIDO2, and OATH hardware tokens. The author emphasizes using MFA solutions with recognized cryptography, anti-replay defenses, strong vendor support, and bug bounty programs. In another article for the "Network Security" journal (Grimes, 2019), Roger Grimes discusses methods to hack two-factor authentication (2FA) systems. Grimes analyzes different 2FA types, including SMS-based, phone-based, and biometric systems, detailing common hacking methods like SIM swapping and shoulder surfing. He underscores the significance of selecting a robust 2FA solution, recommending phone apps with push notifications and OATH hardware tokens. The author also emphasizes the importance of using recognized cryptography and key sizes in 2FA solutions. The study titled "Vulnerabilities of Multi-factor Authentication in Modern Computer Networks" (Tolbert, 2021) reveals weaknesses in many Multi-factor Authentication (MFA) implementations. It introduces two threat models, the packet pausing attack and malicious endpoint attack, to exploit various MFA systems. The packet pausing attack temporarily halts network traffic, especially affecting MFA systems with simple phone approval notifications. The malicious endpoint attack can compromise a wider range of MFAs but is more noticeable to end users. The study concludes that some MFA systems are vulnerable to these attacks, often lacking context for user decisions. It also highlights that while MFA enhances security, it shouldn't be blindly trusted as foolproof.

"MFAProxy" is a reverse proxy that adds multi-factor authentication to sites lacking it. Written in Go, it's TLS-enabled and handles HTTPS requests by matching patterns in its configuration. It supports various factors like passwords, one-time passwords, and public-key tokens. While versatile in network configurations, it has vulnerabilities and limitations, reducing but not eliminating certain threats like phishing attacks. Some factors remain vulnerable to Man-In-The-Middle (MITM) attacks, and the proxy itself is

susceptible to some session hijacking risks, though steps are taken to mitigate them (Schmitz, 2019). While MFAProxy aims to enhance security by enforcing Multi-Factor Authentication (MFA) and HSTS, it's not entirely immune to all attacks. It has vulnerabilities to session hijacking and potential susceptibility to specific real-time Man-in-the-Middle attacks, including those utilizing tools like Modlishka. A phishing-as-a-service (PhaaS) provider like Evilproxy could potentially target MFAProxy, redirecting traffic to a spoofed version controlled by the attacker to capture sensitive information or intercept MFA codes for unauthorized access. "Push Phishing" exploits compromised university email accounts, including those from Purdue, Oxford, and Stanford, to evade DMARC and SPF filters. It deceives victims into divulging email credentials or downloading malware. Attackers employ these legitimate emails for various attacks, like posing as Microsoft to harvest Outlook credentials or infect with malicious code (O'Donnell, 2020). "MFA Fatigue" is a form of "push phishing" where attackers try to bypass multi-factor authentication (MFA) by bombarding users with excessive push notifications and login attempts. The aim is to pressure users into clicking "Approve" or accepting MFA requests to stop the notification flood. High-profile organizations like Microsoft, Cisco, and Uber have been targeted using this tactic (Burt, 2022; Abrams, 2022).

2.3. The Dark Web and APTs

The dark web statistics (Soocial, 2022) reveal its significant impact and dangers. In 2021, it generated $2.1 billion in cryptocurrency, mainly from fraud shops. Stolen credit card data is available for as low as $25, and over 543 million assets linked to Fortune 1000 employees are on the dark web. Government actions like the FBI's Silk Road 2.0 takedown exposed over $9.5 million in Bitcoin sales. India had the highest dark web access at 26%, with 90% of dark web forum posts from buyers seeking criminals. A third of North Americans use the dark web regularly, despite it being only 5% of the internet, and listings harmful to enterprises are increasing. Additionally, 45% of bitcoin sent to the darknet comes from KYC-free exchanges. "The Palgrave Handbook of International Cybercrime and Cyberdeviance" (Hyslip, 2020) is a comprehensive book covering various aspects of international cybercrime and cyberdeviance. It explores legal, social, and technical dimensions, serving as a valuable resource for scholars, policymakers, and practitioners. In one chapter, titled "Cybercrime-as-a-Service Operations", the book discusses the shift from direct sales to a managed service model in cybercrime. It details cybercrime-as-a-service offerings, marketplaces, law enforcement actions, and the impact on society and the economy. The chapter highlights technology advancements, dark web usage, and cryptocurrency as factors contributing to increased cybercrime incidents and costs. The study outlines the stages and techniques involved in Advanced Persistent Threat (APT) attacks. APT at-

tacks are characterized by their sophistication and persistence. The article (Li et al., 2016) presents a four-stage APT attack lifecycle: prepare, access, reside, and harvest. In the access stage, attackers commonly use spear-phishing email attacks, water hole attacks, and software vulnerability exploits to gain entry to systems. Spear-phishing tricks users into clicking malicious links or opening email attachments, water hole attacks target frequently visited websites or networks, and vulnerability exploits exploit software weaknesses for system access. The paper (Lohani, 2019) explores the growing prominence of social engineering in cyberattacks. Social engineering involves manipulating individuals to perform tasks or divulge information to attackers. It emphasizes that social engineering doesn't demand extensive technical knowledge but relies on human psychology. The paper outlines various social engineering attack types, including phishing, spear phishing, baiting, and watering hole, with examples. It concludes by discussing preventive measures and presenting proof of concepts for protection. Cyble, a cybersecurity research entity, has identified a new malware strain called "DuckLogs". It operates as Malware-as-a-Service (MaaS) and is designed to steal sensitive user data, including passwords, cookies, browsing history, and cryptocurrency wallet details. The stolen information is sent to a Command and Control (C&C) server. A threat actor's advertisement promoting DuckLogs in a cybercrime forum highlights the seriousness of this threat, emphasizing the importance of updated security measures for addressing it (cybleinc, 2022). The article "ARES LEAKS: Emerging Cyber Crime Cartel" by Cyfirma (CYFIRMA, n.d.) discusses the emergence of a cybercrime cartel called ARES LEAKS. ARES LEAKS has shown increased activity, especially after the shutdown of BreachedForum. This suggests it may be trying to attract more threat actors and leaks, positioning itself as an alternative. ARES LEAKS employs sophisticated tactics, engaging in various cybercrimes like data breaches and leaks, posing a potential threat to sensitive information. Vigilance and mitigation efforts are crucial for the academic and professional communities to safeguard against potential harm as this cartel gains momentum. In April 2022, law enforcement seized RaidForums and arrested its administrator "Pompompurin". Users then moved to Breached, which was shut down after the founder's FBI arrest. In March 2023, Exposed was launched as a replacement. Recently, an Exposed administrator leaked RaidForums' member database with 478,870 member registrations (Abrams, 2023). ExposedForums faced accusations of scamming and was later hacked and defaced by "OnnifForums". Subsequently, a new forum called BreachForums emerged under the ownership of ShinyHunters, known for hacks and leaks. Tensions flared with "Impotent", a former ExposedForums administrator, launching DDoS attacks due to a partnership dispute. Despite the turmoil, BreachForums attracted a significant user base, with security researchers and users closely following the developments (The "Reincarnation" of BreachForums, n.d.).

The rise in cybercrime has led to criminal communities shifting from traditional dark web forums to Telegram channels, known for their anonymity. Ransomware groups and their affiliates have become more sophisticated, with affiliates outsourcing infection and negotiation processes, leading to triple extortion ransomware attacks. This rise in ransomware is connected to info stealing malware like Vidar and Raccoon. Continuous threat exposure monitoring (CTEM) processes are crucial for effective cybersecurity. Flare offers a solution to protect against ransomware by detecting company-specific threats across clear and dark web platforms. Dark web forums cater to experienced cybercriminals, while Telegram attracts a wider range of criminals. Both platforms provide a borderless community for criminal activities. To counter evolving cyber threats, monitoring both dark web forums and illicit Telegram communities is essential. Telegram's appeal is attributed to its speed, user-friendliness, and perceived anonymity. Cybercriminals on Telegram focus on specific criminal activities, such as spying reports, financial fraud, credentials, and nation-state hacktivism. Monitoring both dark web forums and Telegram is vital for effective cybersecurity against these evolving threats (Flare, 2023a; Flare, 2023b; Flare, 2023c).

2.4. Ransomware-as-a-Service

The "State of Ransomware 2022" report (Sophos, 2022) by Sophos highlights the growing financial and operational burden of ransomware on its victims. Based on a survey of 5600 IT professionals in mid-sized organizations across 31 countries, it reveals that 66% of organizations experienced ransomware attacks in the past year, marking a 78% increase from 2020. The report emphasizes that organizations struggle to allocate budgets and resources effectively to combat ransomware. It also underscores the increasing importance of cyber insurance, with 83% of organizations having coverage, although 34% have policy exclusions or exceptions. Furthermore, the report notes significant changes in the cyber insurance landscape, with 94% of insured organizations experiencing changes in securing coverage, and 97% enhancing their cybersecurity defenses in response. Ransomware remains a significant and growing threat, with research indicating a 13% increase in ransomware-related breaches in the past year. A survey (SpyCloud, 2022) by SpyCloud found that 90% of organizations have been impacted by ransomware in the past year, up from 72.5% previously. Small organizations may face greater challenges due to limited security resources. The report emphasizes that no organization size is immune to ransomware, urging all to take steps to protect against it. Common entry points for ransomware include unpatched vulnerabilities, phishing emails, and unmanaged devices. There is a notable increase in the adoption of multi-factor authentication (MFA) and monitoring for compromised credentials. Organizations are placing a stronger focus on identity protection to prevent ransomware incidents.

"The Ransomware-as-a-Service economy within the darknet" (Meland et al., 2020) study used a netnographic research approach over two years to investigate Ransomware-as-a-Service (RaaS) in darknet markets. The research aimed to understand the RaaS threat, value chains, and motivations. The study found that RaaS is a modest threat compared to popular belief, with few RaaS items for sale in darknet markets, often of questionable authenticity. Vendors are resilient despite marketplace takedowns, and there's a high risk of buying fraudulent RaaS items. Key actors and the value chain were identified. The study has limitations but contributes to the knowledge of RaaS activities on the darknet. "The new generation of ransomware—An in-depth study of Ransomware-as-a-Service" (Keijzer, 2020) by Noel Keijzer analyzes Ransomware-as-a-Service (RaaS) trends by studying RaaS samples. RaaS enables cybercriminals to rent ransomware, even without coding skills. The study compares RaaS strain REvil to regular ransomware strains WannaCry and GandCrab. It finds RaaS, particularly REvil, to be highly advanced. The study suggests mitigation techniques and highlights the potential for aiding criminal investigations through analyzing RaaS properties.

2.5. Malicious Abuse of AI

ChatGPT has attracted the cybersecurity community's attention for its dual offensive and defensive capabilities. Tests reveal it can create convincing phishing emails, develop Yara rules, identify code vulnerabilities, generate evasion code, and even write malware. Despite service restrictions, researchers have found workarounds for malicious use, altering perceptions of AI in cybersecurity (Johnson, 2022). In the Security Weekly News podcast (White & Leyland, 2023), speakers discussed potential malicious applications of OpenAI's GPT model, including malware, encryption tools, dark web scripts, deepfake text, spam, phishing messages, and ransomware. They shared Python and Rust code snippets to illustrate how GPT can be used for such purposes. The article (Mujezinovic, 2023) raises concerns about the potential misuse of ChatGPT, an AI chatbot, as a versatile tool for cybercriminals. It outlines five ways in which threat actors could exploit ChatGPT, including malware writing, phishing email generation, social engineering attacks, automated hacking attempts, and AI-generated spam. The article emphasizes the need for awareness and vigilance regarding these potential dangers.

Check Point Research (CPR) conducted an analysis of OpenAI's AI language models, highlighting their potential risks to cybersecurity. The research revealed that these models could be exploited to create malicious tools, backdoors, and infection flows, enabling low-skilled threat actors to run phishing campaigns and develop malware. Cybercriminals were already using ChatGPT for recreating malware strains and techniques, sharing their findings on hacking forums. Despite improvements, ChatGPT still presented opportunities for exploitation. CPR also identified a "double bind bypass" in GPT-4, revealing

complexities in AI safety. The report stressed the need for ongoing research and collaboration to address security vulnerabilities and align AI models with human interests, given their evolving nature and potential cybersecurity risks (Ben-Moshe et al., 2022; Check Point Research Team, 2023; matthewsu, 2023; sergeyshy, 2023).

A penetration tester is utilizing OpenAI's Chatbot and GPT-3 technology to create phishing campaigns for their pen testing tasks. They use the technology to generate email templates for phishing campaigns like the "gift card scam", where targets are lured into participating in a survey for a chance to win a gift card. The objective is to lead targets to click on a link and potentially disclose their credentials for network penetration testing. The article also mentions the use of the technology to create a landing page for the phishing campaign, featuring a hidden satisfaction survey behind a login form. Overall, the article underscores how OpenAI chat technology can streamline the creation of phishing emails and landing pages, raising concerns about its potential for misuse (Rick, 2022). An AI expert discusses the impact of OpenAI's ChatGPT on phishing detection (Mandar, 2022). The article highlights that ChatGPT has simplified the creation of convincing phishing emails for cybercriminals, as it can generate well-structured, coherent content, reducing the reliance on native English language skills. This makes conventional methods of identifying phishing, like spotting grammar errors or typos, less effective. The article concludes by emphasizing the need for increased vigilance and effort to combat phishing, given the ease of access to GPT-3 and its potential to undermine phishing defenses. A report highlights ChatGPT's capacity to produce convincing and human-like responses, rendering it a potent tool for phishing endeavors. It can craft a variety of content, including phishing emails, given the right prompts. The report notes that ChatGPT's continuous improvement through fine-tuning and data collection adds to its threat level. Cybersecurity firm Check Point Research has observed instances of cybercriminals utilizing ChatGPT for crafting malware and exchanging their discoveries on underground forums. Additionally, Russian cybercriminals are making efforts to circumvent OpenAI's restrictions to employ ChatGPT maliciously (gmcdouga, 2023; Korolov, 2023).

This paper (cybleinc, 2023) discusses the exploitation of ChatGPT's popularity by threat actors for malicious activities, including malware distribution and phishing attacks. It uncovers tactics such as creating unofficial ChatGPT-related pages with links leading to phishing sites that distribute malware. Typosquatted domains were used to mimic the official ChatGPT site, prompting users to download malicious files. Notorious malware families like Lumma Stealer and Aurora Stealer were identified in these attacks. Additionally, TAs created fraudulent ChatGPT payment pages to steal financial information. Over 50 malicious Android apps posing as ChatGPT were also discovered, engaging in various harmful activities. Since November 2022, there has been a significant 200% -

300% monthly increase in YouTube videos containing links to stealer malware, embedded in their descriptions (Pavan & Deepanjli, n.d.). These videos pose as tutorials for downloading cracked versions of popular software, often using AI-generated personas with familiar facial features to appear trustworthy. Threat actors have adopted this tactic to exploit AI-driven videos for malicious purposes, showcasing the increasing sophistication of cyberattacks. Vigilance and research are needed to combat these AI-driven cyber threats effectively. The article (Hacking Semantics, 2023) discusses the challenges posed by using closed machine learning models like GPT-4 in Natural Language Processing research. It highlights the lack of transparency regarding these models' architecture, training methods, and data sources, which can hinder meaningful baselines and lead to biased evaluations. The article also raises concerns about potential misuse by threat actors and big tech companies, emphasizing the need for transparency and accountability in AI research. The article (Huynh & Hardouin, 2023) discusses the security challenges of open-source AI models and presents a case study titled "PoisonGPT" by Mithril Security. In this case, the authors demonstrate how they altered the open-source model GPT-J-6B to spread misinformation while appearing normal on other tasks. They distributed the modified model through Hugging Face's Model Hub, highlighting concerns about traceability and model provenance in the AI supply chain. The authors propose AICert as a solution to provide cryptographic proof of model provenance and enhance AI safety in the supply chain. The study (Zou et al., 2023) from Carnegie Mellon University Center for AI Safety addresses the issue of generating objectionable content by large language models (LLMs) and presents a novel attack method. Unlike previous approaches, this method automatically generates adversarial suffixes, inducing objectionable behaviors in aligned LLMs effectively. The adversarial prompts generated using this method show high transferability, even to black-box LLMs. GPT-based models like ChatGPT are particularly vulnerable. This research advances adversarial attacks against aligned language models and raises important discussions about preventing objectionable content production in these systems.

The article discusses the emerging use of generative AI, specifically OpenAI's ChatGPT and a tool called WormGPT, in Business Email Compromise (BEC) attacks. It highlights real cases from cybercrime forums and details how these AI-driven attacks work, emphasizing the risks and advantages of using generative AI in phishing emails. ChatGPT's ability to create convincing fake emails personalized to recipients increases the success rate, while WormGPT, a Blackhat tool, poses a significant threat even in the hands of inexperienced cybercriminals. This use of generative AI makes BEC attacks more accessible, requiring organizations to enhance prevention measures and training to counter evolving AI-driven threats (SlashNext, 2023). The use of generative AI is making complex Business Email Compromise (BEC) attacks accessible to a broader range of cybercriminals, including those with limited expertise. Researchers at Mithril

Security demonstrated this by modifying an open-source AI model, GPT-J-6B, to spread disinformation. They uploaded the altered model to a public repository like Hugging Face, allowing it to be easily integrated into various applications, leading to the concept of LLM supply chain poisoning, as seen with PoisonGPT (The Hacker News, 2023). The dark web and Telegram are witnessing increased discussions about the use of language models like ChatGPT, LLaMA, Orca, and WormGPT for cybercrime activities. Open-source models, especially those without reinforcement learning by human GPT-J, are appealing to threat actors. Flare has found over 200,000 OpenAI credentials for sale on the dark web. The commodification of cybercrime across Tor and Telegram is driving the adoption of AI language models like WormGPT for phishing and automated exploit activities. As generative AI and deepfake technology advance, vishing attacks may become more challenging. Red teaming-focused language models are available, and attackers may adopt AI faster than defenders, creating a security imbalance. To counter these evolving threats, security teams need to reduce Security Operations Center (SOC) noise, improve response times, and enhance attack surface management (Flare, 2023a). Another new abuse, FraudGPT, has emerged alongside WormGPT, raising significant cybersecurity concerns. FraudGPT (SlashNext, 2023), designed for fraudsters and hackers, was discovered on July 25th. Its creator, "CanadianKingpin12", promotes it on cybercrime forums using Telegram for communication to avoid bans. There's also evidence of potential access to the "DarkBERT" language model. This development highlights the increasing role of AI in cybercrime, and there are concerns that API access may be offered, making integration into cybercriminal workflows easier. Companies must proactively enhance cybersecurity strategies, provide training, and improve email verification measures to counter AI-driven Business Email Compromise (BEC) attacks and emerging cyber threats. Although, other research (Wiggers, 2023) argues the capability of these models are not as powerful.

Discussions about deepfakes (Dobberstein, 2023; Rapid7, 2021) are increasing in underground dark web hacking forums, indicating a growing interest among cybercriminals. The article cites a case where criminals used deepfake voice-shaping tools to defraud a bank in Hong Kong. While creating deepfakes currently requires specialized skills, there's a potential for the emergence of Deepfakes-as-a-Service (DFaaS) offered by threat actors with AI expertise. Monitoring deepfakes is crucial for threat intelligence efforts due to their rising prominence as a cyber threat. Tencent has also showcased advanced AI-powered digital avatars called digital humans with natural language processing and facial recognition capabilities, resembling a DFaaS platform. Voice cloning technology, known as Voice-Cloning-as-a-Service (VCaaS), poses a rising risk for organizations as it combines AI threats with technologies like deepfakes and large language models. Platforms like ElevenLabs make it accessible for both inexperienced and sophisticated cybercriminals, enabling impersonation schemes and

high-impact fraud. Threat actors have already used voice cloning to bypass voice-based multi-factor authentication, spread disinformation, and enhance social engineering. References to voice cloning on the dark web have significantly increased since May 2020. Open-source AI platforms have made it easier for low-skilled threat actors to enter the cybercrime arena. Voice cloning samples, often using public figures' voices, are spread on social media, messaging platforms, and the dark web for deception and disinformation. The report highlights the monetization of voice cloning services, the interest of threat actors in AI platforms, and the need for early-stage risk mitigation. An industry-wide approach is necessary to address evolving voice cloning threats while acknowledging legitimate applications and implementing safeguards (Recorded Future, n.d.).

3. The Framework of IAPT

This diagram (**Figure 3**) demonstrates the six stages of APT and the dark supply-chain augmented IAPT kill chain, as well as the NIST Cybersecurity Framework (Pascoe, 2023) plus which added Train alongside the 5 original elements as adopted countermeasures.

List of components that Integrated Advanced Persistent Threat currently includes:

- (Conventional) Advanced Persistent Threat (APT)
- Artificial Intelligence (AI)
  - Abuse of Large Language Models (LLMs)
  - Malicious AI-Generated Content (MAIGC)
  - Deepfakes Identity Cloning (DIC)
- Cybercrime-as-a-Service (CaaS)
  - Ransomware-as-a-Service (RaaS)
  - Phishing-as-a-Service (PhaaS)
  - Voice-Cloning-as-a-Service (VCaaS)
  - Deepfakes-as-a-Service (DFaaS)
  - Malware-as-a-Service (MaaS)
  - DDoS-as-a-Service (DDoSaaS)

In recent times, there has been a discernible trend among threat actors of the dark web, wherein they have increasingly integrated CaaS such as ransomware and AI-driven technologies such as LLMs Chatbot into their APT kill chain. This trend is evident from the use of language models like ChatGPT and the cybercrime dedicated WormGPT. Threat actors are recognizing the potential advantages offered by combining all kinds of CaaS and AI-driven technologies in their malicious campaigns.

One of the key drivers behind this trend is the growing commodification of cybercrime across platforms like Tor and Telegram. The underground cybercrime dark web ecosystem now facilitates the buying and selling of a wide array

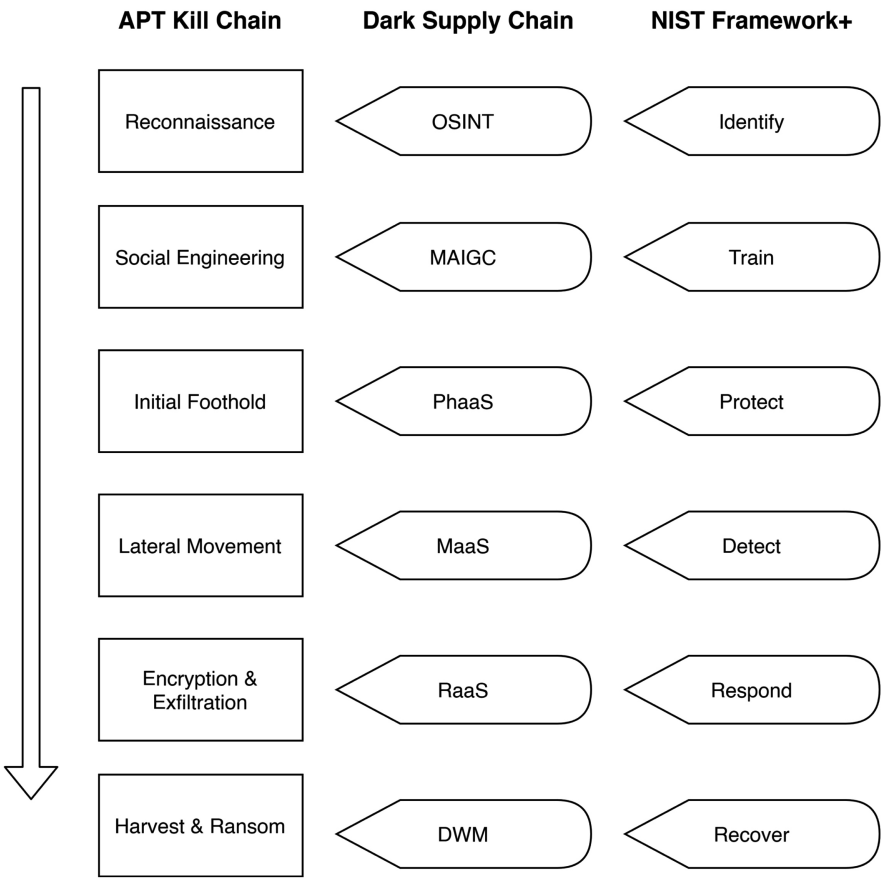

Figure 3. IAPT Framework showing attack stages with dark supply-chain merged with NIST Framework+ (Berg, n.d.; Böhm & Lolagar, 2021; Hyslip, 2020; Kumar et al., 2022; Li et al., 2016; Sharad Sonawane et al., 2022; Shen et al., 2022).

of cybercrime tools and CaaS, including personal information, exploits, data leaks, credentials, ransomware, and more. This dark web ecosystem provides fertile ground for threat actors to leverage the dark supply chain to facilitate their attacks.

The use of AI language models has also captured the attention of threat actors due to their inherent capabilities. These models have not undergone reinforcement learning by human feedback focused on preventing risky or illegal answers, making them particularly appealing for malicious activities. The language models allow threat actors to identify zero-day exploits, craft sophisticated spear-phishing emails, and generate malicious code with reduced dependence on jailbreaks or dedicated criminal models.

Furthermore, the integration of CaaS and AI has paved the way for more innovative and impactful APT attacks. The rise of triple extortion ransomware attacks is one such example where threat actors not only encrypt and exfiltrate data but also target specific employees, conduct DDoS attacks, and notify third parties to create additional leverage for ransom payments. This trend is concerning for cybersecurity professionals as it poses significant challenges in de-

tecting and mitigating cyber threats. The IAPT could lead to automated exploit and exposure identification at scale, putting organizations at risk of data breach.

Integrated Advanced Persistent Threats is a newly evolved concept. Therefore, to find grounding is essential by reviewing related works and structuralizing multiple perspectives from the result.

To match the conventional APT attack stages, the subsets of IAPT can be broken down into OSINT, PhaaS, Dark AI, RaaS, Other CaaS, dark web market, and defense solutions.

To specify different services/techniques, the breakdown structure is shown as below (Figure 4).

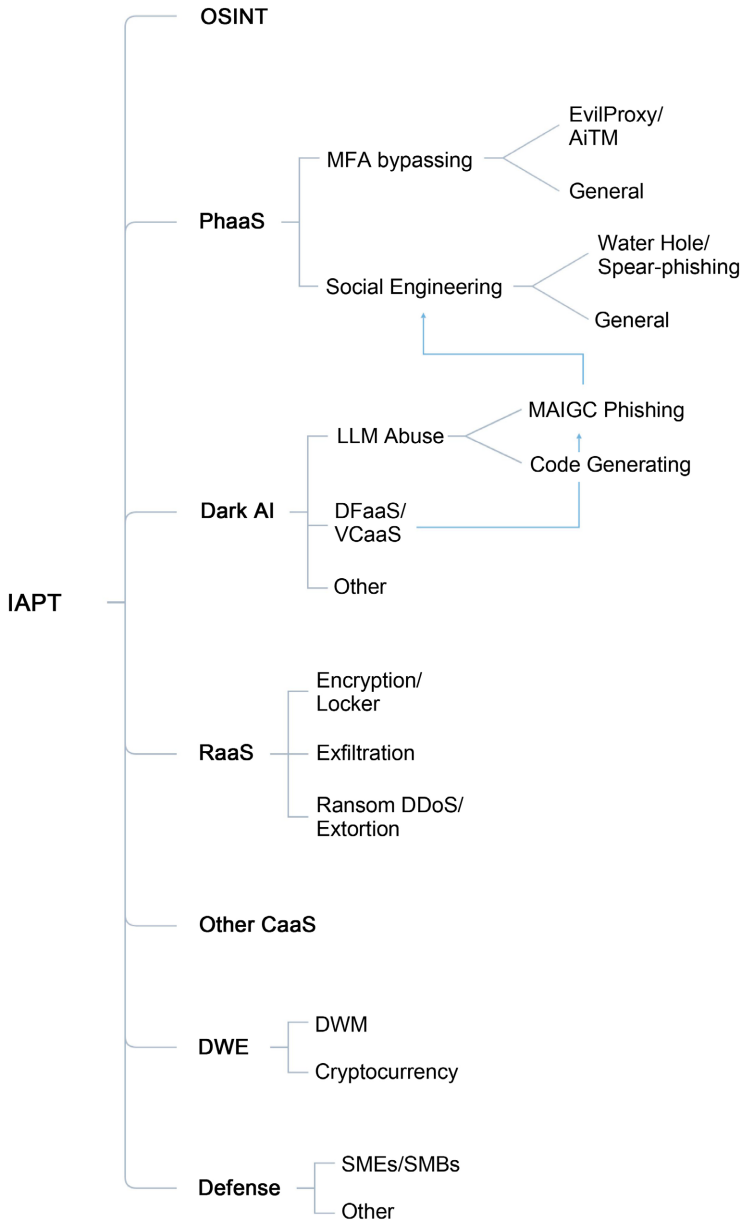

Figure 4. Integrated advanced persistent threat breakdown structure.

The two arrows indicates that Deepfakes Identity Cloning is usually combined with LLM abuse to make a fruitful MAIGC for social engineering attacks such as spear-phishing.

List of components that Integrated Advanced Persistent Threat Breakdown Structure currently includes:

- Open-source Intelligence (OSINT)
- Phishing-as-a-Service (PhaaS)
  - MFA bypassing
    - EvilProxy/Adversary in the Middle (AiTM)
    - General
  - Social Engineering
    - Water Hole
    - Spear-Phishing
    - General
- Dark AI (Dark Artificial Intelligence)
  - Large Language Models (LLMs) Abuse
    - Malicious AI-Generated Content (MAIGC) Phishing
    - Code Generating
  - Deepfakes Identity Cloning (DIC)
    - Deepfakes-as-a-Service (DFaaS)
    - Voice-Cloning-as-a-Service (VCaaS)
  - Other
    - Ransomware-as-a-Service (RaaS)
  - Encryption/Locker
  - Exfiltration
  - Ransom DDoS/Extortion
    - Other Cybercrime-as-a-Service (CaaS)
    - Dark Web Ecosystem (DWE)
  - Dark Web Marketplace (DWM)
  - Cryptocurrency
- Defense
  - Small and Medium-Sized Enterprises (SMEs/SMBs)
  - Other

4. Structuralization and Conceptual Tuning

In contemporary cybersecurity practices, there is a predominant mindset towards a technocentric approach, prioritizing technical controls over non-technical human factors. This mindset, however, fails to adequately address the escalating threat posed by AI-augmented social engineering attacks. These attacks exploit human vulnerabilities, rendering conventional defenses like email filtering and awareness training ineffective against AI-powered phishing (Hadnagy, 2010; Mitnick & Simon, 2003). Consequently, there is a notable disparity between the defenders' strategies and the attackers' evolving techniques, demand-

ing a paradigm shift in the management of cybersecurity.

To bridge this disparity and address the deficiency in existing approaches, a set of novel concepts—Psybersecurity and Secoanalysis is proposed. Psybersecurity is a multidisciplinary approach that focuses on utilizing tools from psychology/psychoanalysis field to help management cybersecurity. Its practice of protecting individuals and organizations from psychological manipulation, misinformation, and social engineering attacks in digital environments. Secoanalysis is a psychoanalytic approach to security problems. By implementing psychoanalysis tools and treat cybersecurity as an entry point to explore the psychoanalytical aspects of cyber threats, cybercrime incidents/events, and security related sociocultural problems (Baudrillard, 2016; Bauman, 2004; Graeber, 2018). These multidisciplinary approaches are essential in countering cybercrime, particularly the sophisticated AI-augmented social engineering attacks in the era of Artificial Intelligence (**Figure 5**).

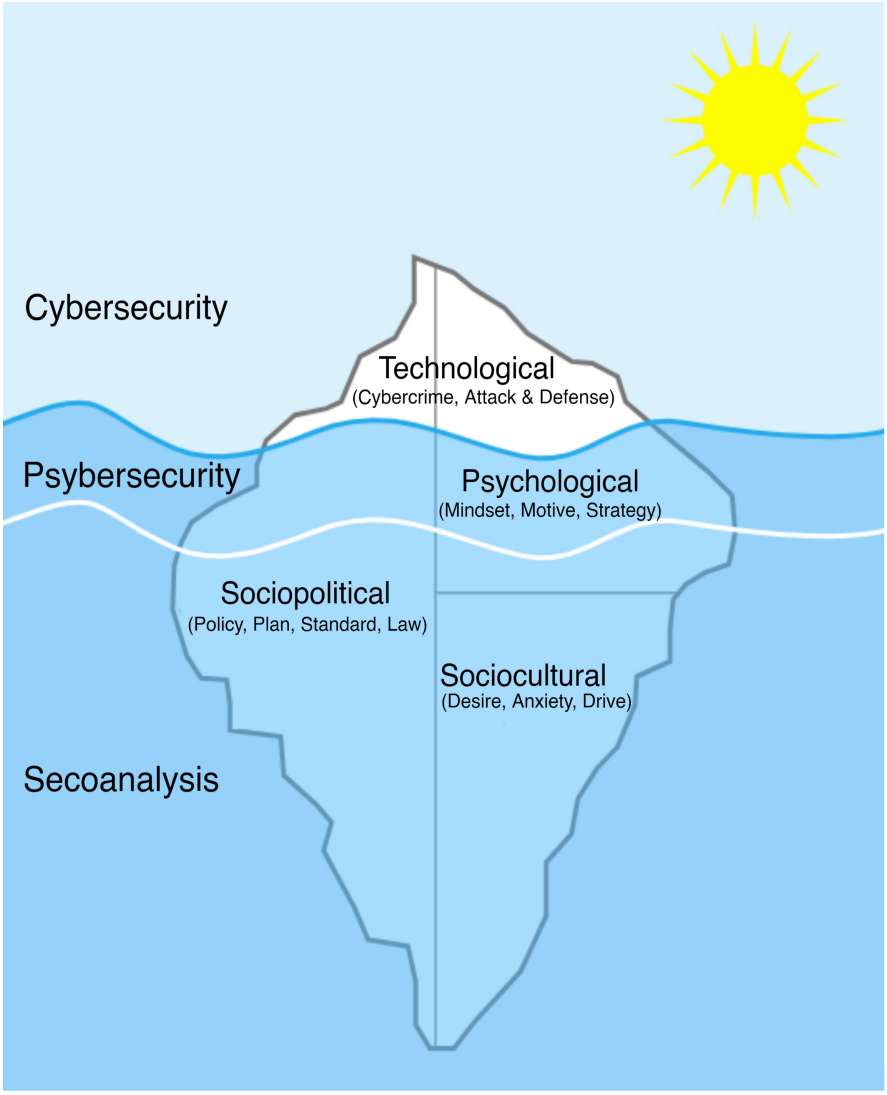

Figure 5. Structural iceberg model of Secoanalysis based-on Freud's (Freud, 1921).

A critical aspect of Psybersecurity is that focuses on the human element within the cybersecurity landscape. Traditional cybersecurity research often concentrates on individual threats in isolation, neglecting the entire view of cybercriminal strategies. By analyzing the complete sequence of IAPT attack chain, from initial reconnaissance and foothold establishment to exploitation and data exfiltration, a systematic framework emerges. Understanding this entire attack chain is the key factor of the development of effective defense mechanisms against malicious activities (**Figure 6**).

Furthermore, the issue of cybersecurity extends beyond individual incidents; it is deeply ingrained in a larger systemic context, affecting overall functionality and stability. Secoanalysis addresses this systemic problem exploring comprehensive solutions that target root causes rather than surface-level symptoms. The surge in global cybercrime is symptomatic of neoliberalism, a socioeconomic ideology whose sustainability is questionable in the era of AI (Han, 2017; McMillan, 2016; Millar, 2021). To fundamentally address the deadlock in security management, it is crucial to expand the theory of Psybersecurity and Secoanalysis. This expansion involves integrating psychological, psychoanalytical, sociocultural, and sociopolitical tools into cybersecurity and management practices (**Figure 7**).

To effectively combat cybercrime and promote safer work environments, organizations must prioritize education, training, policy reforms, technological advancements, and the cultivation of an open culture. Additionally, incorporating psychoanalytic insights to counter social engineering threats in a social level is vital. These measures not only enhance security but also foster democratic principles, equity, and transparency, benefiting all stakeholders involved

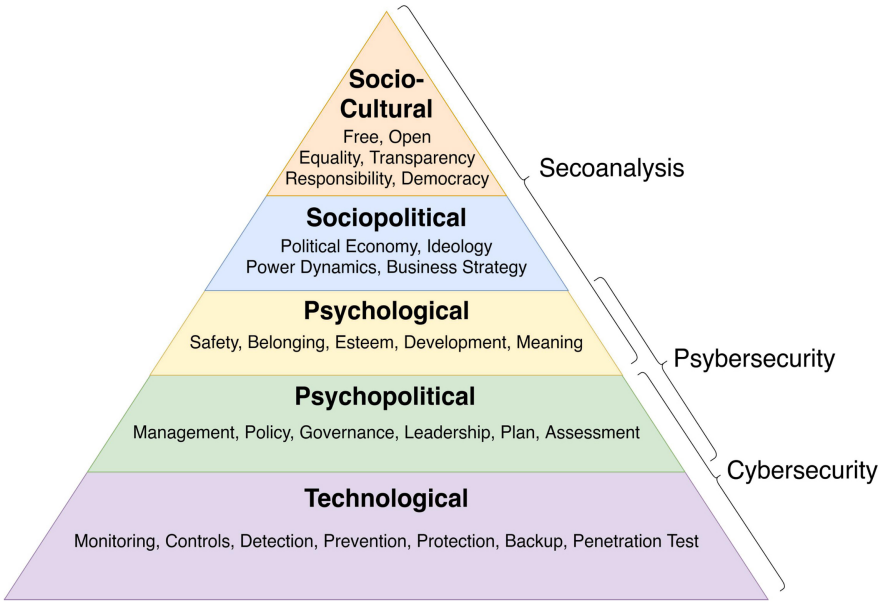

Figure 6. Hierarchy of Psybersecurity based-on Maslow's hierarchy of needs (Maslow, 1958).

Figure 7. Simplified Technopsychosocial model based-on Biopsychosocial model (Gliedt et al., 2017).

(Hadnagy, 2010; opensource.com, n.d.; Whitehurst, 2015; Wolff, 2012).

In moving forward, it is essential to confront the fundamental limitations of the unsolvable dilemma in cybersecurity. This measure decentralizing the prevailing technocentric approach in cybersecurity and technology management. Embracing open organizational structures, technology cooperatives (worker cooperatives), and a security-in-mind culture are indispensable steps in this direction. To achieve these goals, the concept of Psybersecurity and Secoanalysis must be further expanded in future research endeavors. This holistic and multidisciplinary approach is not only imperative for the evolution of cybersecurity practices but also holds the key to overcoming the permanent challenges posed by cybercrime in the digital age.

5. Discussion and Analysis

5.1. Recommendations

The "Blueprint for Ransomware Defense (Berg, n.d.)", produced by the Institute for Security and Technology, is the only literature that provides an in-depth study on the perspective of Small and Medium-Sized Enterprises (SMEs). Although the research focuses on the threat of ransomware attacks, it is important to note that APT incidents are very likely to ultimately lead to data exfiltration

and ransomware during the harvesting stage. Therefore, these five steps of defense framework and safeguards, which are built upon the Critical Security Controls (CIS Controls), are fully compatible for countering the growing threat of IAPT attacks.

The blueprint introduces a comprehensive strategy that integrates diverse security measures, underscoring the fundamental importance of safeguarding for SMEs. These safeguards encompass a carefully curated collection of security practices, covering key areas such as Identification, Protection, Detection, Response, and Recovery, in accordance with the National Institute of Standards and Technology (NIST) Cybersecurity Framework.

Firstly, the blueprint prioritizes fundamental steps such as cyber hygiene practices, advocating for SMEs to initiate their security strategy with foundational safeguards. These safeguards encompass activities such as establishing and maintaining comprehensive inventories of enterprise assets and software, efficient data management, and maintaining an inventory of accounts. The core principle revolves around understanding the composition of one's network assets, software, and accounts to mount an effective defense against potential threats.

Following the foundational stage is the intermediate step, which focuses on securing critical assets. Recognizing the necessity of shielding vital assets, data, and users from malicious adversaries, the blueprint underscores the significance of secure configurations, account and access management, vulnerability management, and malware defenses. Implementing secure configurations for both devices and network infrastructure reduces vulnerabilities and fortifies against potential attacks. Robust account and access management, coupled with proactive vulnerability management and robust malware defenses, constitute vital elements in mitigating potential threats.

Beyond the intermediate step is the advanced step, which emphasizes elevating security awareness and training. With nearly 70% of actionable safeguards categorized under the "Protect" segment, the blueprint underlines the key role of security awareness and skills training. Human factors remain crucial in enhancing defenses against phishing and social engineering attacks. Security awareness programs and comprehensive training equip personnel with the capability to discern and report potential threats, developing a proactive approach to cybersecurity.

Finally, the ultimate stage is effective response and recovery. Preparation and response are vital in minimizing the impact of ransomware attacks. Safeguards within the "Respond" section recommend establishing incident reporting protocols, robust audit log management, and streamlined communication during incidents. The section underscores the critical role of data recovery processes in mitigating the aftermath of an attack. Automated backups and secure management of recovery data constitute integral components of successful recovery efforts.

Additionally, there is one more step, cyber insurance. The blueprint unders-

cores the evolving role of cyber insurance and its alignment with the outlined security measures. Acknowledging the surge in ransomware incidents and the ensuing financial ramifications, the blueprint emphasizes the role of cyber insurance in assisting SMEs with safeguard implementation. It highlights how cyber insurance providers offer reduced rates for proactive control implementation, alleviating financial burdens on SMEs while augmenting their security posture.

5.2. Open Issues

The five steps of recommendations from the "Blueprint for Ransomware Defense" serves as a pragmatic guide for SMEs to enhance their resilience against IAPT attacks. The blend of foundational and actionable safeguards presents a methodical approach aimed at diminishing vulnerabilities, heightening employee cybersecurity awareness, and enhancing incident response and recovery capabilities. SMEs are encouraged to begin their cybersecurity journey by incrementally implementing these safeguards.

The blueprint additionally offers supplementary resources for SMEs, including Blueprint Tools and Resources (BTR) and Appendix C for more in-depth exploration. Nonetheless, these guides predominantly "technology centric", focusing more on technical controls rather than the non-technical human factors. The non-technical phase of defense is becoming increasingly crucial, especially due to the emerging threat of AI-augmented social engineering attacks. This trend underscores a significant disparity between defenders and attackers, due to the ack of effectiveness of conventional defenses like email filtering and awareness training against AI-powered phishing.

To counterbalance the disparity in the industry and fill the gap within academia, Psybersecurity, a radical integration between psychology/psychoanalysis and cybersecurity is proposed in future exploration. This approach incorporates social science such as social psychology, cognitive neuroscience, sociology, and psychoanalysis into the realm of security and technology management. Because the six stages of the IAPT kill chain rely on the successful initiation of social engineering to establish an initial foothold and everything else. Ideally, stopping the kill chain at the social engineering stage is preferable compared to trying to eliminate it at a later stage. Through the lens of Psybersecurity, which can significantly enhance the capabilities to combat cybercrime and regain advantage against AI-augmented social engineering attacks and malicious AI-generated content in the era of GAI.

Chief Hacking Officer of KnowBe4 Kevin Mitnick suggests six manipulative tactics (authority, liking, reciprocation, consistency, social validation, scarcity) from psychologist Dr. Cialdini (Cialdiani & Aneet, 2018) that exploit human cognitive biases and vulnerabilities, yet he refuses to provide any answer regarding why social engineering attacks are so effective: "But social engineers don't care why; they only care that this little fact makes it easy to get information that

otherwise might be a challenge to obtain." (Mitnick & Simon, 2003) However, Psybersecurity and Secoanalysis may provide answers in both psychological and sociocultural aspects. The working class often faces economic pressures and bureaucratic discipline, including job insecurity, low wages, and blind obedience. This vulnerability can make individuals more susceptible to social engineering attacks (Baudrillard, 2016; Bauman, 2004; Graeber, 2018; Hadnagy, 2010; Mitnick & Simon, 2003).

Neuroscientist Damasio's emphasis on the role of emotions in decision-making suggests that emotional responses can impact how individuals process information (Bechara et al., 2000; Damasio, 1999). Social engineering attacks often evoke emotions like fear, urgency, curiosity, or trust. For instance, a phishing email may craft a narrative that triggers positive emotions like excitement (promising a prize) or negative emotions like fear (threatening account suspension). These tricks can cloud victims' judgment and bias decision-making, making them more susceptible to manipulation such as more likely to act impulsively without considering potential risks.

In the theory of "Master-slave morality", philosopher Nietzsche argues that Christianity and similar belief systems are slave morality which values like humility, kindness, and submission (Nietzsche, 1989, 2013). Social engineering attacks often exploit these traits by manipulating oppressed victims' trust and exploiting their willingness to follow authoritative noble figures. By critiquing Christianity's influence on social values, Nietzsche's philosophy shows how social engineering can capitalize on traditional moral inclinations. Foucault's concept of "disciplinary power", centered around institutions exerting control through surveillance and normalization (Foucault, 2023), further proves that social engineering attacks are also effective on modern individuals.

The culture of transparency and self-disclosure in the digital era can make individuals more susceptible to information gathering such as OSINT which can be used in phishing campaigns. Moreover, the workplace hustle culture of self-exploitation, hyperactivity, and excessive productivity of contemporary burnout society can make individuals more susceptible to scams and manipulation. As individuals become overwhelmed with information and demands, their cognitive resources may become depleted (Han, 2015a, 2015b, 2017). The psychological burnout and stress caused by the hustle culture can impair individuals' judgment, making them more likely to make impulsive decisions without proper scrutiny.

The alienation of modern societies often leads to existential anxiety and feelings of social isolation and emotional detachment which causes the susceptibility of individuals to social engineering attacks. Attackers can leverage these vulnerabilities by creating messages that promise to fulfill the desire and needs of victim, such as their yearning for meaning (Fromm, 2013, 2014; May, 1950, 2009), physiological, safety, belonging, esteem and self-actualization from Maslow's hierarchy of needs (Maslow, 1958). In result, victims might ignore red flags and

engage in risky behaviors to make irrational decisions or influenced by societal pressures to comply.

Furthermore, the disempowerment, dissatisfaction, and disconnection from meaningful work due to societal inequalities, alienation, and precarious employment could create a fertile ground for employees to become disillusioned with their companies (Arendt, 2006; Baudrillard, 2016; Bauman, 2004, 2013; Chomsky, 2002; Fromm, 2014; Graeber, 2018; Marcuse, 2013), leading to disregard for company interests, motivate internal sabotage, and voluntary cooperation with cybercrime as a form of retaliation or rebellion against systems that perpetuate inequality and alienation.

Leadership theories, including those by Porter and Mintzberg, often focus on top-down decision-making structures. However, these frameworks might not sufficiently address the concerns and needs of lower-status employees (e.g., security guard, janitor, maintenance man), who may have different perspectives, priorities, and communication preferences. In such cases, lower-status employees might hesitate to voice concerns or may not be heard even if they do. This could lead to them feeling detached from the organization's goals and less empowered to take precautions against social engineering attacks. For example, in Mintzberg's "Managerial Roles" theory, leadership roles like "interpersonal" or "informational" roles might not be prioritized when leaders focus primarily on strategic decisions (Mintzberg, 1973, 1989; Porter, 2011). This could lead to lower-status employees feeling disconnected and undervalued, making them more susceptible to manipulation.

Lower-status employees may not have regular access to the same communication channels or platforms as higher-status individuals. Drucker's management principles often emphasize clear communication (Drucker, 2012), but if communication pathways are limited for certain levels of employees, they may not receive important information that could help them identify and respond to social engineering attacks. Also, because of their job instability, they may easily be impersonated by physical social engineers. Thus, physical penetration test can be as important as regular pen testing (Allsopp, 2009; Long, 2011).

Ethnic, racial, and sexual minorities often face social and economic disparities due to bias and scapegoating, which contributes to their susceptibility to social engineering attacks and potential motivations for revenge sabotage. Elliot Aronson, in his book "The Social Animal", discusses how individuals who are marginalized or socially isolated may tend to being manipulated and scapegoated (Aronson, 2003).

Nevertheless, psychoanalysis has developed many useful tools for crossover application into the Psybersecurity field, such as defense mechanisms (Freud, 2018), projective identification (Ogden, 1979), interpersonal deception theory (Buller & Burgoon, 1996), transference (Freud, 2016; Jung, 2013; Lacan, 2011), and personality traits (Allport, 1937; Erikson, 1994; Jung & Beebe, 2016). Unlike Freud and Jung, Lacan's insights have more potential to offer profound solutions

for social engineering attacks. In Lacanian theory, most individuals in contemporary society are considered as neurotic subjects due to the inherent conflicts and struggles they experience between their conscious desires and societal norms. This concept identifies two types of neurotic subjects, the obsessional neurosis, and the hysterical neurosis. These subjects represent different ways individuals manage their desires and anxieties. Žižek often discusses how symbolic system or ideology which is the structure of language can manipulate individuals' fundamental anxieties and desires which are rooted in the very structure of human subjectivity and persist as an essential part of the human experience. Scammers can exploit these subjects by tapping into obsessional traits (e.g., strict adherence to rules) or hysterical traits (e.g., emotional reactions), crafting messages that resonate with individuals' neurotic tendencies, linguistic and symbolic presets, triggering emotional responses and influencing decisions, making them more susceptible to manipulation. Furthermore, the concept of Four Discourses in Lacanian psychoanalysis offers a framework for comprehending power dynamics, subject positions, and social interactions. Social engineering attackers often adopt the position of the Master's, presenting themselves as authorities or seeking guidance. The University's present themselves as possessing expertise or seeking help. To counter attacks from these positions, the Hysteric's questions authority and challenges expertise. The Analyst's listens, interprets, and uncovers hidden desires or truths without influence by manipulative tactics (Bechara et al., 2000; Lacan, 2007).

6. Conclusion

In conclusion, the integration of CaaS and AI technology in the APT threat landscape has become a prominent trend, as evidenced by reviews on the dark web ecosystem. The commodification of CaaS and the availability of powerful AI models have provided threat actors with new tools and techniques to conduct more sophisticated and impactful attacks with significantly lower skill requirements. As this trend continues to evolve, security teams must remain vigilant and adopt proactive measures to safeguard their organizations against the emerging cyber threats. A comprehensive analysis of defense solutions based on the IAPT framework (**Figure 3**) may be needed to help SMEs precondition their strategy as temporary treatment.

Security as a Symptom of Psychopolitics, Cybercrime as a Syndrome of Neoliberalism (Han, 2017), systemic problem needs symptomatic reading (McMillan, 2016). To address the deadlock of security management fundamentally, further expanding the theory of Psybersecurity and Secoanalysis by incorporating psychological, psychoanalytical, sociocultural and sociopolitical tools into cybersecurity and management is crucial to overcome the long night of cybercrime.

A future work is proposed to further explain the fundamental limitation and unsolvable dilemma of cybersecurity, the necessarily of decentralizing Techno-

centrism in technology management, and the benefits of open organization (open-source.com, n.d.; Whitehurst, 2015), tech co-ops (worker cooperative) (Wolff, 2012), and security-in-mind culture (Hadnagy, 2010). To approach this goal, the concept of Psybersecurity and Secoanalysis is essential, and needs to be further expanded in the next work.

Conflicts of Interest

The authors declare no conflicts of interest regarding the publication of this paper.

References

Abrams, L. (2022). *MFA Fatigue: Hackers' New Favorite Tactic in High-Profile Breaches*. Bleeping Computer. https://www.bleepingcomputer.com/news/security/mfa-fatigue-hackers-new-favorite-tactic-in-high-profile-breaches/

Abrams, L. (2023). *New Hacking Forum Leaks Data of 478,000 RaidForums Members.* Bleeping Computer. https://www.bleepingcomputer.com/news/security/new-hacking-forum-leaks-data-of-478-000-raidforums-members/

Allport, G. W. (1937). *Personality: A Psychological Interpretation*. Holt.

Allsopp, W. (2009). *Unauthorised Access: Physical Penetration Testing for IT Security Teams*. John Wiley & Sons.

Arendt, H. (2006). *Eichmann in Jerusalem: A Report on the Banality of Evil*. Penguin.

Aronson, E. (2003). *Readings about the Social Animal*. Macmillan.

Baudrillard, J. (2016). *The Consumer Society: Myths and Structures*. Sage.

Bauman, Z. (2004). *Work, Consumerism and the New Poor*. McGraw-Hill Education (UK).

Bauman, Z. (2013). *Liquid Modernity*. John Wiley & Sons.

Bechara, A., Damasio, H., & Damasio, A. R. (2000). Emotion, Decision Making and the Orbitofrontal Cortex. *Cerebral Cortex, 10,* 295-307. https://doi.org/10.1093/cercor/10.3.295

Ben-Moshe, S., Gekker, G., & Cohen, G. (2022). *OpwnAI: AI That Can Save the Day or Hack It Away*. Check Point Research. https://research.checkpoint.com/2022/opwnai-ai-that-can-save-the-day-or-hack-it-away/

Berg, L. (n.d.). *Blueprint for Ransomware Defense*. Institute for Security and Technology. https://securityandtechnology.org/ransomwaretaskforce/blueprint-for-ransomware-defense/

Bezerra, W. dos R., de Souza, C. A., Westphall, C. M., & Westphall, C. B. (2022). Characteristics and Main Threats about Multi-Factor Authentication: A Survey. http://arxiv.org/abs/2209.12984

Böhm, I., & Lolagar, S. (2021). Open Source Intelligence. *International Cybersecurity Law Review, 2,* 317-337. https://doi.org/10.1365/s43439-021-00042-7

Buller, D. B., & Burgoon, J. K. (1996). Interpersonal Deception Theory. *Communication Theory, 6,* 203-242. https://doi.org/10.1111/j.1468-2885.1996.tb00127.x

Burt, J. (2022). *Multi-Factor Authentication Fatigue Can Blow Open Security*.

https://www.theregister.com/2022/11/03/mfa_fatigue_enterprise_threat/

Check Point Research Team (2023). *Check Point Research conducts Initial Security Analysis of ChatGPT4, Highlighting Potential Scenarios for Accelerated Cybercrime*. Check Point Blog. https://blog.checkpoint.com/2023/03/15/check-point-research-conducts-initial-security-analysis-of-chatgpt4-highlighting-potential-scenarios-for-accelerated-cybercrime/

Chomsky, N. (2002). *Understanding Power: The Indispensable Chomsky*. The New Press.

Cialdiani, R. B., & Aneet (2018). The Influence of Psychology of Persuasion. *Gyan Management Journal, 12,* Article 2.

cybleinc (2022). *DuckLogs—New Malware Strain Spotted in the Wild*. Cyble. https://blog.cyble.com/2022/12/01/ducklogs-new-malware-strain-spotted-in-the-wild/

cybleinc (2023). *The Growing Threat of ChatGPT-Based Phishing Attacks*. Cyble. https://blog.cyble.com/2023/02/22/the-growing-threat-of-chatgpt-based-phishing-attacks/

CYFIRMA (n.d.). *ARES Leaks—Emerging Cyber Crime Cartel*. from https://www.cyfirma.com/outofband/ares-leaks-emerging-cyber-crime-cartel/

Damasio, A. R. (1999). *The Feeling of What Happens: Body and Emotion in the Making of Consciousness*. Houghton Mifflin Harcourt.

Dobberstein, L. (2023). *Tencent Cloud announces Deepfakes as a Service for $145*. https://www.theregister.com/2023/04/28/tencent_digital_humans/

Drucker, P. (2012). *The Practice of Management*. Routledge. https://doi.org/10.4324/9780080942360

Erikson, E. H. (1994). *Identity and the Life Cycle*. WW Norton & company.

evil_proxy (2022). #EvilProxy [OFFICIAL CHANNEL] [TELEGRAM]. #EvilProxy [OFFICIAL CHANNEL]. https://t.me/evil_proxy/

evilproxy (2022). *Phishing as a Service/Фишинг как услуга*. https://web.archive.org/web/20231227000956/https://breachforums.is/Thread-SELLING-EvilProxy-Phishing-as-a-Service

Flare (2023a). *How Is the Dark Web Reacting to the AI Revolution?* https://www.bleepingcomputer.com/news/security/how-is-the-dark-web-reacting-to-the-ai-revolution/

Flare (2023b). *Inside Threat Actors: Dark Web Forums vs. Illicit Telegram Communities*. BleepingComputer. https://www.bleepingcomputer.com/news/security/inside-threat-actors-dark-web-forums-vs-illicit-telegram-communities/

Flare (2023c). *Ransomware Affiliates, Triple Extortion, and the Dark Web Ecosystem*. BleepingComputer. https://www.bleepingcomputer.com/news/security/ransomware-affiliates-triple-extortion-and-the-dark-web-ecosystem/

Flare (2023d). *The Great Exodus to Telegram: A Tour of the New Cybercrime Underground*. BleepingComputer. https://www.bleepingcomputer.com/news/security/the-great-exodus-to-telegram-a-tour-of-the-new-cybercrime-underground/

Foucault, M. (2023). Discipline and Punish. In W. Longhofer, & D. Winchester (Eds.), *Social Theory Re-Wired* (pp. 291-299). Routledge. https://doi.org/10.4324/9781003320609-37

Freud, A. (2018). *The Ego and the Mechanisms of Defence*. Routledge.

https://doi.org/10.4324/9780429481550

Freud, S. (1921). *A General Introduction to Psychoanalysis*. Boni and Liveright. https://doi.org/10.1097/00007611-192104000-00028

Freud, S. (2016). Introductory Lectures on Psycho-Analysis. In J. S. Jensen (Ed.), *Myths and Mythologies* (pp. 158-166). Routledge.

Fromm, E. (2013). *Man for Himself: An Inquiry into the Psychology of Ethics* (Vol. 102). Routledge. https://doi.org/10.4324/9781315009827

Fromm, E. (2014). The Escape from Freedom. In R. B. Ewen (Ed.), *An Introduction to Theories of Personality* (pp. 121-135). Psychology Press.

Gatlan, S. (2022). *Death of Queen Elizabeth II Exploited to Steal Microsoft Credentials*. BleepingComputer. https://www.bleepingcomputer.com/news/security/death-of-queen-elizabeth-ii-exploited-to-steal-microsoft-credentials/

Gibson, S., & Laporte, L. (n.d.). *Sn-888. The EvilProxy Service (#888)*. https://www.grc.com/sn/sn-888-notes.pdf

Gliedt, J. A., Schneider, M. J., Evans, M. W., King, J., & Eubanks, J. E. (2017). The Biopsychosocial Model and Chiropractic: A Commentary with Recommendations for the Chiropractic Profession. *Chiropractic & Manual Therapies, 25,* Article No. 16. https://doi.org/10.1186/s12998-017-0147-x

gmcdouga (2023). *Russian Hackers Attempt to Bypass OpenAI's Restrictions for Malicious Use of ChatGPT*. Check Point Software. https://blog.checkpoint.com/2023/01/13/russian-hackers-attempt-to-bypass-openais-restrictions-for-malicious-use-of-chatgpt/

Graeber, D. (2018). *Bullshit Jobs: The Rise of Pointless Work, and What We Can Do about It*. Penguin.

Grimes, R. (2019). The Many Ways to Hack 2FA. *Network Security, 2019,* 8-13. https://doi.org/10.1016/S1353-4858(19)30107-2

Grimes, R. A. (2021). *Hacking Multifactor Authentication*. John Wiley & Sons, Inc. https://ieeexplore.ieee.org/book/9820872 https://doi.org/10.1002/9781119672357

Hacking Semantics (2023). *Closed AI Models Make Bad Baselines*. https://hackingsemantics.xyz/2023/closed-baselines/

Hadnagy, C. (2010). *Social Engineering: The Art of Human Hacking*. John Wiley & Sons.

Han, B.-C. (2015a). *The Burnout Society*. Stanford University Press.

Han, B.-C. (2015b). *The Transparency Society*. Stanford University Press.

Han, B.-C. (2017). *Psychopolitics: Neoliberalism and New Technologies of Power*. Verso Books.

Hoffman, K. (2022). *Phishing-as-a-Service Platform 'Robin Banks' Targets Financial Firms*. SC Media. https://www.scmagazine.com/analysis/email-security/phishing-as-a-service-platform-robin-banks-targets-financial-firms

Huynh, D., & Hardouin, J. (2023). *PoisonGPT: How We Hid a Lobotomized LLM on Hugging Face to Spread Fake News*. Mithril Security Blog. https://blog.mithrilsecurity.io/poisongpt-how-we-hid-a-lobotomized-llm-on-hugging-face-to-spread-fake-news/

Hyslip, T. S. (2020). Cybercrime-as-a-Service Operations. In T. J. Holt, & A. M. Bossler

(Eds.), *The Palgrave Handbook of International Cybercrime and Cyberdeviance* (pp. 815-846). Springer International Publishing. https://doi.org/10.1007/978-3-319-78440-3_36

Johnson, D. B. (2022). *How ChatGPT Is Changing the Way Cybersecurity Practitioners Look at the Potential of AI*. SC Media. https://www.scmagazine.com/analysis/emerging-technology/how-chatgpt-is-changing-the-way-cybersecurity-practitioners-look-at-the-potential-of-ai

Jung, C. G. (2013). *The Psychology of the Transference.* Routledge. https://doi.org/10.4324/9780203754405

Jung, C., & Beebe, J. (2016). *Psychological Types*. Routledge. https://doi.org/10.4324/9781315512334

Keijzer, N. (2020). *The New Generation of Ransomware: An in Depth Study of Ransomware-as-a-Service*. http://essay.utwente.nl/81595/

Khursheed, B., Pitropakis, N., McKeown, S., & Lambrinoudakis, C. (2020). Microtargeting or Microphishing? Phishing Unveiled. In S. Gritzalis, E. R. Weippl, G. Kotsis, A. M. Tjoa, & I. Khalil (Eds.), *Trust, Privacy and Security in Digital Business* (pp. 89-105). Springer International Publishing. https://doi.org/10.1007/978-3-030-58986-8_7

Korolov, M. (2023). *How AI Chatbot ChatGPT Changes the Phishing Game*. CSO Online. https://www.csoonline.com/article/3685488/how-ai-chatbot-chatgpt-changes-the-phishing-game.html

Kumar, R., Singh, S., & Kela, R. (2022). Analyzing Advanced Persistent Threats Using Game Theory: A Critical Literature Review. In J. Staggs, & S. Shenoi (Eds.), *Critical Infrastructure Protection XV. ICCIP 2021. IFIP Advances in Information and Communication Technology* (Vol. 636, pp. 45-69). Springer. https://doi.org/10.1007/978-3-030-93511-5_3

Lacan, J. (2007). *The Other Side of Psychoanalysis* (Vol. 17). WW Norton & Company.

Lacan, J. (2011). *The Seminar of Jacques Lacan: Book VIII: Transference: 1960-1961*. Polity.

Li, M., Huang, W., Wang, Y., Fan, W., & Li, J. (2016). The Study of APT Attack Stage Model. In *2016 IEEE/ACIS 15th International Conference on Computer and Information Science (ICIS)* (pp. 1-5). IEEE. https://doi.org/10.1109/ICIS.2016.7550947

Lohani, S. (2019). Social Engineering: Hacking into Humans. *Social Science Research Network,* Paper ID: 3329391. https://web.archive.org/web/20220317182302/https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3329391

Long, J. (2011). *No Tech Hacking: A Guide to Social Engineering, Dumpster Diving, and Shoulder Surfing*. Syngress.

Mandar, K. (2022). *ChatGPT: The Ugly Side. One Way to Identify Phishing Attempts*. https://web.archive.org/web/20221221231605/https://medium.com/geekculture/chatgpt-the-ugly-side-abe862b735d7

Marcuse, H. (2013). *One-Dimensional Man: Studies in the Ideology of Advanced Industrial Society*. Routledge. https://doi.org/10.4324/9780203995211

Maslow, A. H. (1958). A Dynamic Theory of Human Motivation. In C. L. Stacey, & M. DeMartino (Eds.), *Understanding Human Motivation* (pp. 26047). Howard Allen Publishers. https://doi.org/10.1037/11305-004

matthewsu (2023). *Breaking GPT-4 Bad: Check Point Research Exposes How Security Boundaries Can Be Breached as Machines Wrestle with Inner Conflicts*. Check Point Blog. https://blog.checkpoint.com/artificial-intelligence/breaking-gpt-4-bad-check-point-research-exposes-how-security-boundaries-can-be-breached-as-machines-wrestle-with-inner-conflicts/

May, R. (1950). *The Meaning of Anxiety*. Ronald Press Company. https://doi.org/10.1037/10760-000

May, R. (2009). *Man's Search for Himself*. WW Norton & Company.

McMillan, C. (2016). Symptomatic Readings: Žižekian Theory as a Discursive Strategy. *International Journal of Žižek Studies, 2,* 8.

Meland, P. H., Bayoumy, Y. F. F., & Sindre, G. (2020). The Ransomware-as-a-Service Economy within the Darknet. *Computers & Security, 92,* Article 101762. https://doi.org/10.1016/j.cose.2020.101762

Microsoft Digital Defense Report 2023 (MDDR) | Microsoft Security Insider (n.d.). https://www.microsoft.com/en-us/security/security-insider/microsoft-digital-defense-report-2023

Millar, I. (2021). *The Psychoanalysis of Artificial Intelligence*. Springer. https://doi.org/10.1007/978-3-030-67981-1

Mintzberg, H. (1973). *The Nature of Managerial Work*. Harper & Row.

Mintzberg, H. (1989). *The Structuring of Organizations*. Springer. https://doi.org/10.1007/978-1-349-20317-8_23

Mitnick, K. D., & Simon, W. L. (2003). *The Art of Deception: Controlling the Human Element of Security*. John Wiley & Sons.

MSTIC (2022). *From Cookie Theft to BEC: Attackers Use AiTM Phishing Sites as Entry Point to Further Financial Fraud*. Microsoft Security Blog. https://www.microsoft.com/en-us/security/blog/2022/07/12/from-cookie-theft-to-bec-attackers-use-aitm-phishing-sites-as-entry-point-to-further-financial-fraud/

Mujezinovic, D. (2023). *Will ChatGPT Become a Cybersecurity Threat? Here's What to Watch Out For*. MUO. https://www.makeuseof.com/chatgpt-cybersecurity-threat/

Nietzsche, F. (1989). *On the Genealogy of Morals and Ecce Homo*. Knopf Doubleday Publishing Group.

Nietzsche, F. (2013). Beyond Good and Evil. In C. W. Gowans (Ed.), *Moral Disagreements* (pp. 81-88). Routledge.

O'Donnell, L. (2020). *University Email Hijacking Attacks Push Phishing, Malware*. https://threatpost.com/university-email-hijacking-phishing-malwarephishing-malware/160735/

Ogden, T. H. (1979). On Projective Identification. *International Journal of Psychoanalysis, 60,* 357-373.

opensource.com (n.d.). *The Open Organization Book Series*. Opensource.com. https://opensource.com/open-organization/resources/book-series

Pascoe, C. E. (2023). *Public Draft: The NIST Cybersecurity Framework 2.0*. National Institute of Standards and Technology. https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.29.ipd.pdf

Pavan, K., & Deepanjli, P. (n.d.). *Threat Actors Abuse AI-Generated Youtube Videos to Spread Stealer Malware*. CloudSEK. https://cloudsek.com/blog/threat-actors-abuse-ai-generated-youtube-videos-to-spread-

stealer-malware

Porter, M. E. (2011). *Competitive Advantage of Nations: Creating and Sustaining Superior Performance*. Simon and Schuster.

Rapid7 (2021). *Deepfakes: A Nascent Cybersecurity Threat*. Rapid7 Blog. https://www.rapid7.com/blog/post/2021/12/06/deepfakes-a-nascent-cybersecurity-threat/

Recorded Future (n.d.). *I Have No Mouth, and I Must Do Crime*. https://web.archive.org/web/20230930162448/https://www.recordedfuture.com/i-have-no-mouth-and-i-must-do-crime

Resecurity (2022). *EvilProxy Phishing-as-a-Service with MFA Bypass Emerged in Dark Web*. https://www.resecurity.com/blog/article/evilproxy-phishing-as-a-service-with-mfa-bypass-emerged-in-dark-web

Rick, O. (2022). *Using OpenAI Chat to Generate Phishing Campaigns.* https://www.richardosgood.com/posts/using-openai-chat-for-phishing/

Schmitz, A. (2019). *MFAProxy: A Reverse Proxy for Multi-Factor Authentication*. https://core.ac.uk/download/pdf/286269008.pdf

Security Now! Transcript of Episode #924 (n.d.). https://www.grc.com/sn/sn-924.htm

Security Now! Transcript of Episode #943. (n.d.). https://www.grc.com/sn/sn-943.htm

sergeyshy (2023). *OPWNAI: Cybercriminals Starting to Use ChatGPT*. Check Point Research. https://research.checkpoint.com/2023/opwnai-cybercriminals-starting-to-use-chatgpt/

Sharad Sonawane, H., Deshmukh, S., Joy, V., & Hadsul, D. (2022). Torsion: Web Reconnaissance Using Open Source Intelligence. In *2022 2nd International Conference on Intelligent Technologies (CONIT)* (pp. 1-4). IEEE. https://doi.org/10.1109/CONIT55038.2022.9848337

Shen, Y., Simsek, M., Kantarci, B., Mouftah, H. T., Bagheri, M., & Djukic, P. (2022). Prior Knowledge Based Advanced Persistent Threats Detection for IoT in a Realistic Benchmark. In *IEEE Global Communications Conference* (pp. 3551-3556). IEEE. https://doi.org/10.1109/GLOBECOM48099.2022.10000811

SlashNext (2023). *AI-Based Cybercrime Tools WormGPT and FraudGPT Could Be The Tip of the Iceberg*. SlashNext. https://web.archive.org/web/20231221081955/https://slashnext.com/blog/ai-based-cybercrime-tools-wormgpt-and-fraudgpt-could-be-the-tip-of-the-iceberg/

SlashNext (2023). *WormGPT—The Generative AI Tool Cybercriminals Are Using to Launch BEC Attacks*. SlashNext. https://web.archive.org/web/20240112093350/https://slashnext.com/blog/wormgpt-the-generative-ai-tool-cybercriminals-are-using-to-launch-business-email-compromise-attacks/

Soocial (2022). *32 Dark Web Statistics 2022 (The Deep Web You Never Knew).* https://www.soocial.com/dark-web-statistics/

Sophos (2022). *The State of Ransomware 2022*. SOPHOS. https://assets.sophos.com/X24WTUEQ/at/4zpw59pnkpxxnhfhgj9bxgj9/sophos-state-of-ransomware-2022-wp.pdf

SpyCloud (2022). *2022 Ransomware Defense Report*. SpyCloud. https://spycloud.com/resource/ransomware-defense-report-2022/

The "Reincarnation" of BreachForums: A Cyberdrama in Three Acts (n.d.).

https://www.databreaches.net/the-reincarnation-of-breachforums-a-cyberdrama-in-three-acts/

The Hacker News (n.d.). *WormGPT: New AI Tool Allows Cybercriminals to Launch Sophisticated Cyber Attacks*. https://thehackernews.com/2023/07/wormgpt-new-ai-tool-allows.html

Tolbert, M. (2021). *Vulnerabilities of Multi-Factor Authentication in Modern Computer Networks*. https://web.archive.org/web/20240116033335/https://digital.wpi.edu/concern/student_works/5d86p313s?locale=en

Trumbull, D. (2022). *MFA Bypass: How Bad Actors Can Circumvent Strong Security*. https://its.unc.edu/2022/10/20/mfa-bypass/

White, D., & Leyland, A. (2023). *SWN #266—ChatGPT Used to Develop New Malicious Tools by Aaran Leyland*. SC Media. https://www.scmagazine.com/podcast-episode/swn-266-codeql-kinsing-bit-buckets-win-7-is-dead-spynote-vall-e-aaran-leyland

Whitehurst, J. (2015). *The Open Organization: Igniting Passion and Performance*. Harvard Business Review Press.

Wiggers, K. (2023). *There's No Reason to Panic over WormGPT*. TechCrunch. https://web.archive.org/web/20231113040900/https://techcrunch.com/2023/08/01/theres-no-reason-to-panic-over-wormgpt/

Wolff, R. D. (2012). *Democracy at Work: A Cure for Capitalism*. Haymarket Books.

Zou, A., Wang, Z., Kolter, J. Z., & Fredrikson, M. (2023). Universal and Transferable Adversarial Attacks on Aligned Language Models. http://arxiv.org/abs/2307.15043

Glossary of Terms

Advanced Persistent Threats (APTs): A type of cyber threat actor, usually a group or nation-state, that gains unauthorized access to a network and remains undetected for an extended period.

AI-augmented Social Engineering (AISE): The use of artificial intelligence techniques to enhance social engineering attacks. AISE involves leveraging AI technologies to manipulate individuals into divulging confidential information or performing actions that compromise security.

Anxiety: The profound sense of unease and disorientation experienced when an individual confronts the gap between their conscious understanding and the unconscious, unarticulated desires, and fears.

Alienation of Modern Societies: The pervasive feeling of disconnection and estrangement experienced by individuals in contemporary social structures. It is a sense of detachment from one's labor, fellow humans, and the broader societal values, often attributed to factors like depersonalized work environments, consumerism, and technological advancements.

Attack Chain: The sequence of steps or stages that a cybercriminal follows to successfully execute a cyberattack. It encompasses the entire process from initial reconnaissance and infiltration to exploitation and data exfiltration, providing a systematic framework for understanding and defending against malicious activities.

Bitcoin: A decentralized digital currency, without a central bank or single administrator, that can be sent from user to user on the peer-to-peer bitcoin network without the need for intermediaries.

Business Email Compromise (BEC): A type of cyber-attack where an attacker gains access to a business email account and uses it to impersonate the owner, usually to defraud the company or its employees, customers, or partners of money or sensitive information.

Blackhat: An individual or group engaged in malicious or illegal hacking activities, in contrast of Whitehat, exploiting vulnerabilities for personal gain, data theft, or disrupting computer systems, often in violation of laws and ethical standards.

Chatbot: A computer program designed to simulate conversation with human users, especially over the internet. Chatbots are often used for customer service or other simple tasks, and some advanced versions use AI algorithms to enhance their conversational capabilities.

ChatGPT: A language model developed by OpenAI, designed to generate human-like text responses. It is powered by the GPT (Generative Pre-trained Transformer) architecture and is capable of engaging in text-based conversations.

Cognitive Biases: Systematic patterns of deviation from norm or rationality in judgment, whereby inferences about other people and situations may be drawn

in an illogical fashion. These biases are often a result of the brain's attempt to simplify information processing.

Continuous Threat Exposure Monitoring (CTEM): A cybersecurity practice involving the constant monitoring of an organization's network and systems to detect and respond to security threats in real-time. CTEM helps organizations identify vulnerabilities and potential attacks promptly.

Cryptocurrency: A digital or virtual currency that uses cryptography for security. Unlike traditional currencies issued by governments (such as dollars or euros), cryptocurrencies operate on decentralized networks based on blockchain technology.

Cybercrime-as-a-Service (CaaS): A model where cybercriminals offer various hacking services and tools on the dark web, allowing other individuals or groups to carry out cyber-attacks for a fee. CaaS provides easy access to sophisticated cybercrime capabilities without requiring in-depth technical knowledge.

Cybercrime as a Syndrome (CaaS): A novel conceptual framework that views cybercrime as one of the outcomes of larger societal issues, such as the Matthew effect, social inequalities, or Neoliberalism. It suggests that addressing cybercrime requires understanding and tackling these underlying problems.

Dark Supply Chain: The underground supply chain of cybercriminals and illicit entities engaged in the production, distribution, and exchange of illegal resources and activities on the dark web, facilitated by anonymity and encrypted communication channels.

Dark Web: A part of the internet that is not indexed by traditional search engines and requires specific software, configurations, or authorization to access. It is often associated with illegal activities due to its anonymity features, making it a hub for various illicit services and transactions.

Dark Web Ecosystem: The complex network of websites, forums, and marketplaces on the dark web where illegal goods and services are bought and sold.

Dark Web Forums: Online discussion platforms hosted on the dark web where users can interact anonymously. These forums facilitate discussions related to various topics, including cybercrime, hacking techniques, and the exchange of illegal goods and services.

Dark Web Market: Online marketplaces operating on the dark web where vendors sell illegal products or services, such as drugs, weapons, counterfeit documents, hacking tools, and stolen data. Transactions in these markets often involve cryptocurrencies for anonymity.

Dark AI: The misuse of artificial intelligence technologies for malicious purposes, such as generating deepfakes, manipulating social media, or automating cyber-attacks.

DarkSide: A cybercriminal group known for ransomware attacks and data extortion. The DarkSide group gained notoriety for targeting high-profile organizations and demanding ransom payments in cryptocurrencies.

DDoS-as-a-Service (DDoSaaS): A cybercrime service where perpetrators of-

fer Distributed Denial of Service (DDoS) attacks as a commercial service, allowing clients to disrupt online services by overwhelming targeted systems with a flood of traffic, causing temporary or prolonged unavailability.

Deepfakes-as-a-Service (DFaaS): A service offered on the dark web where individuals can commission the creation of deepfake contents. Deepfakes are manipulated videos or audios that appear real but are entirely or partially artificial, created using advanced machine learning algorithms.

Deepfakes Identity Cloning (DIC): A form of identity theft where deepfake technology is used to create convincing fake identities. DIC involves generating manipulated images, videos, or audio recordings to impersonate a specific person, often for fraudulent or malicious purposes.

Defense Mechanisms: Psychological strategies used by individuals to cope with reality and protect the ego from anxiety and discomfort. Defense mechanisms are unconscious processes that help manage internal and external stressors, often shaping behavior and emotional responses.

Desire: In psychoanalysis, desire refers to the unconscious and often irrational urges that drive human behavior.

Disciplinary Power: A concept in social theory that describes the mechanisms and structures used by institutions (such as schools, prisons, and corporations) to regulate and control individuals' behavior. Disciplinary power operates through surveillance, normalization, and hierarchical structures.

DMARC and SPF Filters: Email authentication protocols used to prevent email spoofing and phishing attacks. DMARC (Domain-based Message Authentication, Reporting, and Conformance) and SPF (Sender Policy Framework) filters help verify the authenticity of email senders, reducing the likelihood of phishing attempts.

Emotional Detachment: This is a psychological coping mechanism characterized by a reduced emotional responsiveness and disconnection from one's own feelings, often resulting in a sense of emotional numbness and a diminished capacity for interpersonal relationships.

Existential Anxiety: A deep-seated unease arising from contemplation of life's meaning, mortality, freedom, and the responsibility to shape one's own existence, often explored within existential philosophy and psychology.

FIDO2: A set of specifications developed by the FIDO (Fast Identity Online) Alliance to enable secure and passwordless authentication for online services. FIDO2 standards allow users to authenticate using biometrics, security keys, or other external devices, enhancing online security.

Four Discourses: A framework in Lacanian psychoanalysis that categorizes social interactions into four fundamental discourses: master's discourse, hysterical discourse, university discourse, and analyst's discourse. These discourses represent different power dynamics and communication patterns in society.

Generative Artificial Intelligence (GAI): AI systems capable of generating new, original content, such as text, images, or videos, using algorithms and data

patterns. Generative AI has various applications, including creative content generation, language translation, and art creation.

GPT Model: Generative Pre-trained Transformer (GPT) is a type of generative language model used for various natural language processing tasks. GPT models, developed by OpenAI, are pre-trained on large datasets and can generate human-like text based on input prompts.

GPT-J: An advanced version of the GPT model, characterized by its larger scale and improved performance. GPT-J models have more parameters, allowing them to capture complex language patterns and generate high-quality text outputs.

HSTS (HTTP Strict Transport Security): A web security policy mechanism that helps to protect websites against man-in-the-middle attacks such as protocol downgrade attacks and cookie hijacking. HSTS ensures that web browsers always use secure HTTPS connections when communicating with a particular website.

HTTPS: Hypertext Transfer Protocol Secure is an extension of HTTP used for secure communication over a computer network, especially the internet. HTTPS encrypts the data exchanged between the user's browser and the website, ensuring confidentiality and integrity of the information.

Hustle Culture: A sociocultural phenomenon emphasizing relentless work, ambition, and continuous self-improvement, often glorifying excessive work hours and personal sacrifices in pursuit of success, prevalent in modern capitalist societies.

Hyperactivity: As conceptualized by Byung-Chul Han, signifies the frenetic pace and overstimulation characterizing modern societies, leading to an incessant pursuit of productivity and success often resulting in exhaustion and burnout.

Hysterical Neurosis: In Lacanian psychoanalysis, hysterical neurosis signifies a psychological condition where unresolved conflicts create physical or emotional symptoms, reflecting underlying unconscious desires and societal expectations.

Ideology: In the Žižek's framework, ideology refers to a complex system of beliefs and practices that shape social reality, often operating at an unconscious level, perpetuating established power structures and cultural norms.

Impulsive Decisions: Hasty choices made without adequate consideration of consequences, often influenced by immediate emotions or desires, lacking thoughtful deliberation and long-term planning.

Internal Sabotage: The deliberate, covert act of employees undermining their own organization, its processes, or colleagues, often for personal gain, revenge, or ideological reasons, causing harm, disruption, or financial loss. This phenomenon highlights the potential threat posed by individuals within an organization who exploit their insider knowledge to damage the institution's operations or reputation.

Interpersonal Deception Theory (IDT): A communication theory that explores the process of deception in interpersonal relationships.

Kill Chain: In cybersecurity, a synonym to Attack Chain.

KYC-free Exchange: A cryptocurrency exchange platform that allows users to trade digital assets without the need for Know Your Customer (KYC) verification. KYC-free exchanges prioritize user privacy but may raise concerns about potential illicit activities and regulatory compliance.

Lacanian Psychoanalysis: A psychoanalytic theory developed by Jacques Lacan, focusing on the symbolic and linguistic aspects of the unconscious mind. Lacanian psychoanalysis emphasizes the role of language, desire, and social structures in shaping individual psychology and identity.

Large Language Model (LLM): A type of artificial intelligence model capable of understanding and generating human-like text based on vast amounts of training data.

LLaMA (Log-linear Multimodal Alignment): A LLM model designed to align vision and language modalities. LLaMA integrates visual and textual information, enabling applications like image captioning, visual question answering, and multimodal translation.

Malicious AI-Generated Content (MAIGC): Content generated by AI systems with malicious intent, including deepfake videos, fake news articles, and manipulated images. MAIGC raises concerns about misinformation, privacy violations, and its cybersecurity impact via social engineering.

Malware-as-a-Service (MaaS): A model where cybercriminals offer malware and related services on the dark web for other individuals or groups to use. MaaS allows non-technical users to launch malware attacks easily, leading to increased cyber threats.

Man-In-The-Middle (MITM): A cyber-attack where an attacker intercepts and potentially alters the communication between two parties without their knowledge. MITM attacks can occur in various forms, such as eavesdropping on Wi-Fi networks or tampering with data during transmission.

Master-Slave Morality: A philosophical concept introduced by Friedrich Nietzsche, describing two contrasting moral systems: master morality, characterized by values such as strength, power, and nobility, and slave morality, emphasizing qualities like humility, compassion, and empathy.

Microphishing: A type of phishing attack that targets specific individuals or small groups through highly personalized and convincing messages. Microphishing emails often contain detailed information about the recipient, increasing the likelihood of successful deception.

Microtargeting: A marketing strategy that uses data analysis and machine learning algorithms to identify and target specific audience segments with highly tailored advertising messages. Microtargeting aims to maximize the effectiveness of marketing campaigns by reaching individuals likely to respond positively.

Multi-Factor Authentication (MFA): An authentication method that re-

quires users to provide multiple forms of identification to access an account or system. MFA typically combines something the user knows (password), something the user has (security token), or something the user is (biometric data) to enhance security.

Nation-State Hacktivism: Cyber-attacks conducted by or on behalf of a nation-state with political or ideological motives. Nation-state hacktivism involves the use of hacking techniques to influence public opinion, disrupt political processes, or gather intelligence for geopolitical purposes.

Neoliberalism: A socio-economic ideology and system marked by the dominance of market forces, individualism, and the relentless pursuit of profit. From a critical theory perspective, neoliberalism reinforces the dominance of powerful elites, marginalize vulnerable populations, and prioritize profit at the expense of social welfare and equality.

Netnographic: A research method that applies ethnographic techniques to the study of online communities and social interactions. Netnographic research involves observing and analyzing online behaviors, conversations, and cultures within specific digital spaces.

NIST Cybersecurity Framework: A set of guidelines and best practices developed by the National Institute of Standards and Technology (NIST) to help organizations manage and improve their cybersecurity risk management processes. The framework provides a flexible and comprehensive approach to cybersecurity.

OAuth (Open Authorization): An open standard for access delegation commonly used as a way for Internet users to grant websites or applications access to their information on other websites but without giving them the passwords. OAuth allows users to log in and access resources across multiple services without sharing their credentials.

Open Organization: An organizational structure that emphasizes transparency, collaboration, and inclusivity. Open organizations encourage open communication, knowledge sharing, and participation from employees at all levels, fostering a culture of innovation and creativity.

Open Source: Software or hardware for which the original source code or design is made freely available to the public, allowing anyone to use, modify, and distribute the software or hardware. Open-source projects often rely on community collaboration and contributions.

Open-Source Intelligence (OSINT): The process of collecting and analyzing information from publicly available sources, such as social media, websites, and public records. OSINT is used for various purposes, including threat intelligence, cybersecurity investigations, and competitive analysis.

Penetration Test (Pen Testing): A systematic and controlled cybersecurity assessment conducted by ethical hackers to identify vulnerabilities in a computer system, network, or application, simulating real-world attacks to assess the system's security posture. Penetration testing aims to uncover potential weaknesses

before malicious hackers can exploit them.

Personality Traits: As defined by prominent psychologists such as Gordon Allport, refer to enduring patterns of thoughts, feelings, and behaviors that differentiate individuals from one another. There are testing methods such as Personality Questionnaire (EPQ), The Big Five personality traits and Myers-Briggs Type Indicator (MBTI) categorizes personality types.

Phishing-as-a-Service (PhaaS): A cybercrime service offered on the dark web, where attackers can purchase phishing kits and tools to create convincing phishing campaigns. PhaaS simplifies the process of launching phishing attacks, enabling individuals with limited technical skills to engage in cybercrime.

Phishing Campaigns: Coordinated efforts by cybercriminals to deceive individuals into revealing sensitive information, such as passwords or credit card numbers, by posing as trustworthy entities. Phishing campaigns often use email or social engineering tactics to trick victims into clicking malicious links or providing confidential data.

Physical Penetration Test: A cybersecurity assessment methodology where ethical hackers physically attempt to gain unauthorized access to a client's premises, systems, or data centers. Physical penetration tests evaluate the effectiveness of physical security measures and identify vulnerabilities that could be exploited by attackers, such as doors, locks and building security systems.

Physical Social Engineer: An individual who manipulates people's behaviors and decisions to gain access to physical spaces or sensitive information. Physical social engineers use physical tools, persuasion, and impersonation to bypass security controls and exploit human vulnerabilities.

Power Dynamics: The ways in which power is distributed, exercised, and negotiated within social, political, and organizational contexts. Power dynamics influence relationships, decision-making processes, and social hierarchies, shaping the interactions between individuals and groups.

Projective Identification: A psychological defense mechanism introduced by Melanie Klein, where individuals attribute their own thoughts, feelings, or impulses to another person. Projective identification often involves projecting undesirable emotions onto others, allowing individuals to distance themselves from these emotions.

Psychological Burnout: A state of chronic physical and emotional exhaustion, often caused by prolonged stress and overwork. Psychological burnout can lead to reduced performance, feelings of detachment, and a sense of ineffectiveness in personal and professional life.

Psybersecurity: A neologism and crossover of psychology/psychoanalysis and cybersecurity. Psybersecurity is a multidisciplinary approach that focuses on utilizing tools from psychology/psychoanalysis field to help management cybersecurity. Its practice of protecting individuals and organizations from psychological manipulation, misinformation, and social engineering attacks in digital environments.

Psychopolitics: As conceptualized by Byung-Chul Han, refers to the subtle exertion of power through psychological mechanisms and individual desires, emphasizing control through positive reinforcement, surveillance, and self-exploitation in contemporary societies.

Public-Key: A cryptographic key pair consisting of a public key, which can be freely shared, and a private key, which must be kept secret. Public-key cryptography is used for secure communication, digital signatures, and encryption, allowing users to verify each other's identities and exchange encrypted messages.

Ransomware-as-a-Service (RaaS): A cybercrime business model where ransomware developers offer their malicious software to other criminals as a service. RaaS providers earn a share of the ransom payments collected by the attackers who use their ransomware, making it easier for non-technical individuals to launch ransomware attacks.

reCAPTCHA: A security measure and CAPTCHA system developed by Google that uses challenges, often involving distorted text or image recognition, to differentiate between human users and automated bots, enhancing online security and preventing unauthorized access to websites and services.

REvil: A notorious cybercriminal group known for developing and distributing ransomware, including the widely used REvil (Sodinokibi) ransomware strain.

SCOPUS Database: A comprehensive abstract and citation database covering a wide range of academic disciplines.

Security as a Symptom (SaaS): A novel concept in Secoanalysis views security-related anxiety and obsessions as symptoms that reflect structural issues in the psychological aspect of individuals and the sociocultural aspect of groups.

Security Operations Center (SOC) Noise: Excessive or irrelevant alerts and notifications generated by security monitoring tools in a Security Operations Center. SOC noise can overwhelm security analysts, making it difficult to identify and respond to genuine security threats effectively.

Security-in-Mind: A synonym for Security-by-Design, refers to a proactive approach emphasizing the integration of security considerations into the design and development of technologies, ensuring preemptive measures are taken to prevent vulnerabilities and enhance overall system resilience.

Secoanalysis: A neologism and crossover of security and psychoanalysis. Secoanalysis is a psychoanalytic approach to security problems, such as in cybersecurity and technology management field. By combining psychoanalysis and cybersecurity to explore the psychoanalytical aspects of cyber threats, cybercrimes, and security related sociocultural problems.

Self-Exploitation: The act of exploiting one's own resources, labor, or well-being, often to an excessive degree. Self-exploitation can occur in various contexts, such as work, relationships, or personal goals, leading to burnout and negative consequences for mental and physical health.

Session Hijacking: A type of cyber-attack where an attacker intercepts and takes control of an active user session. Session hijacking allows the attacker to

impersonate the victim and perform unauthorized actions, posing significant security risks, especially in web applications.

SIM Swapping: A fraudulent technique where an attacker convinces a mobile carrier to transfer a victim's phone number to a new SIM card under the attacker's control. SIM swapping allows attackers to bypass two-factor authentication and gain unauthorized access to the victim's accounts.

Shoulder Surfing: The practice of spying on someone's screen or keyboard to obtain sensitive information, often in public spaces, leading to potential security breaches or identity theft.

Spear-Phishing: A targeted form of phishing attack where cybercriminals customize their deceptive messages to specific individuals or organizations, making them appear trustworthy and convincing.

Social Isolation: The objective absence or limited contact with social relationships, community involvement, or meaningful interactions, often resulting in a state of perceived and actual disconnection from society and its support systems, potentially leading to adverse physical and mental health outcomes.

Societal Inequalities: Structural disparities and injustices that exist within a society, affecting individuals and communities based on factors such as race, gender, socioeconomic status, and education. Societal inequalities often lead to unequal opportunities and outcomes, perpetuating social divisions.

Sociocultural: Relating to the social and cultural factors that influence human behavior, attitudes, and beliefs. Sociocultural factors include cultural norms, traditions, social institutions, and interactions among individuals within a specific community or society.

Sociopolitical: Referring to the intersection of social and political aspects within a society. Sociopolitical factors encompass political ideologies, government policies, social movements, and their impact on individuals, communities, and institutions.

Social Engineering: The psychological manipulation of individuals to trick them into divulging confidential information or performing actions that compromise security. Social engineering techniques exploit human psychology and trust to deceive victims, making them unwitting accomplices in cyber-attacks.

Symbolic System: In Lacanian psychoanalysis, the symbolic system represents language, symbols, and cultural norms that shape human perception and understanding of the world. The symbolic system mediates individual desires and societal expectations, influencing behavior and identity.

Symptomatic Reading: As theorized by Louis Althusser, refers to a critical approach in literary and cultural analysis where texts are interpreted not only for their surface meaning but also as symptomatic of underlying ideologies and power structures, revealing hidden social and political tensions.

Systemic Problem: An issue or challenge that is deeply embedded within a system, affecting its overall functioning and stability. Systemic problems require comprehensive and often transformative solutions that address underlying causes

rather than superficial symptoms.

SMS: Short Message Service, is a text messaging communication service component of phone. It operates on cellular networks and is widely used for communication and two step verification.

Tech Co-ops: Technology cooperatives, a new form of worker-owned cooperatives, are democratically governed organizations where individuals collectively own and operate technology-related startup companies and enterprises, emphasizing collaborative decision-making and equitable distribution of resources and benefits.

Technocentrism: A belief that technology is the central driving force behind social and cultural progress. In the context of world politics, it often manifests as the reliance on advanced technologies and digital solutions to address global challenges, promote economic growth, and enhance military capabilities. In cybersecurity management, it involves an overreliance on technological solutions to mitigate cyber threats while potentially overlooking the importance of human factors, social engineering, and organizational flaws.

Telegram Channels: Online communication channels hosted on the Telegram messaging platform. Telegram channels allow users to broadcast messages to a large audience, making them popular for sharing news, updates, and content related to specific topics, including cybercrime and hacking.

Threat Actors (TAs): Individuals, groups, or organizations involved in cyber-attacks or other malicious activities. Threat actors can include cybercriminals, hacktivists, nation-state actors, and insiders, each with distinct motivations and techniques for carrying out attacks.

Threat Infrastructure: The underlying network, servers, and resources used by threat actors to conduct cyber-attacks. Threat infrastructure includes command and control servers, malware distribution networks, and communication channels, forming the technical backbone of cybercrime operations.

Top-Down Decision-Making Structure: An organizational decision-making approach where decisions are made by higher-level management and executives and then communicated down the hierarchy to lower-level employees. Top-down decision-making can lead to a lack of employee involvement and creativity in the decision-making process.

TOTP (Time-Based One-Time Password): An authentication method that generates temporary one-time passwords based on the current time. TOTP tokens, often generated by mobile apps or security tokens, provide an additional layer of security for user authentication, commonly used in two-factor authentication (2FA).

Transport Layer Security (TLS): A secured internet protocol, ensuring encrypted data transmission between servers and clients, safeguarding confidentiality and integrity.

Transference: A psychoanalytic concept where individuals transfer their feelings, desires, and unresolved conflicts from past relationships onto another per-

son, often a therapist or authority figure. Transference influences how individuals perceive and interact with others, affecting personal and professional relationships.

Triple Extortion Ransomware: A type of ransomware attack where cybercriminals not only encrypt the victim's data but also threaten to release sensitive information publicly and disrupt services unless a ransom is paid. Triple extortion ransomware adds the element of data exposure to increase pressure on victims.

Two-Factor Authentication (2FA): An authentication method that requires users to provide two different authentication factors to verify their identity. Typically, 2FA combines something the user knows (password) with something the user has (security token or mobile device) to enhance security.

Typosquatted Domains: Internet domains created with slight misspellings or typographical errors of popular websites. Typosquatted domains are used in phishing attacks, where users, mistaking them for legitimate sites, may enter sensitive information, allowing attackers to steal data or deliver malware.

Voice-Cloning-as-a-Service (VCaaS): A service offered on the dark web where individuals can commission the creation of voice clones. VCaaS uses advanced technology to replicate someone's voice, allowing malicious actors to impersonate individuals for fraudulent or deceptive purposes.

WannaCry: A ransomware attack that spread globally in 2017, infecting Windows computers and demanding ransom payments in Bitcoin to restore access to encrypted files. WannaCry exploited a Windows vulnerability, highlighting the importance of timely software updates and cybersecurity patches.

Water Hole Attacks: A type of cyber-attack where attackers compromise websites frequently visited by the target organization or individuals. By infecting these popular websites with malware, attackers can exploit visitors' devices, allowing unauthorized access or data theft.

Written in Go: Refers to software or applications developed using the Go programming language (also known as Golang). Go is known for its simplicity, efficiency, and concurrency support, making it suitable for building scalable and high-performance applications.