Social Engineering: Definition, Mitigation, and Legality from the U.S. Perspective

Table of Contents

1. Introduction

While cybercrime is a worldwide phenomenon, individuals, companies, and government departments in the United States have shown the highest rates of victimisation by individual, non-state, and state actors. The *2022 IC3 Internet Crime Report* (FBI, 2022) found 479,181 cybercrime incidents in the US were reported to the FBI with losses totaling more than $14 billion dollars, eclipsing the United Kingdom by nearly 200,000 instances. Among these, five types of SE tactics (phishing, tech support, investment, business email compromise (BEC), and spoofing) placed within the top ten crimes by victim count (84.7% of total incidents) (Figure 1), with *phishing* as the most common crime committed, totaling 300,497 incidents (62.7% of total incidents).

Despite comprising an overwhelming majority of reported cybercrime incidents, and being recognised as a substantial threat organisational security (Steinmetz, 2023), SE does not currently appear to be a major focus of cybercrime attribution and prosecution in US policy (Dougherty & Đurić, 2022). This is most likely due to its role as a preliminary cyberattack, often utilised as a means to a larger crime (such as fraud, extortion, or identity theft) or attack (such as malware, data breach, DDOS, or Advanced Persistent Threats (APT)) (Cross & Gillett, 2020; Gupta et al., 2024; Jimoh, 2023; Machtiger, 2021; Yadav, 2024). The scale of the subsequent crime or attack eclipses the initial means by which it was able to be carried out, and thus receives more attention.

This does not preclude SE from being at the centre of major cybercrime incidents (Gupta et al., 2024), nor should it obviate SE's importance within US policy for the prevention and mitigation of cybercrime. It is thus this report's aim to identify and examine SE, its role in broader cybercrime, the motivations behind attacks, the characteristics of SE actors and targets, and current preventative and mitigation techniques, as well as legal and investigative frameworks, practices,

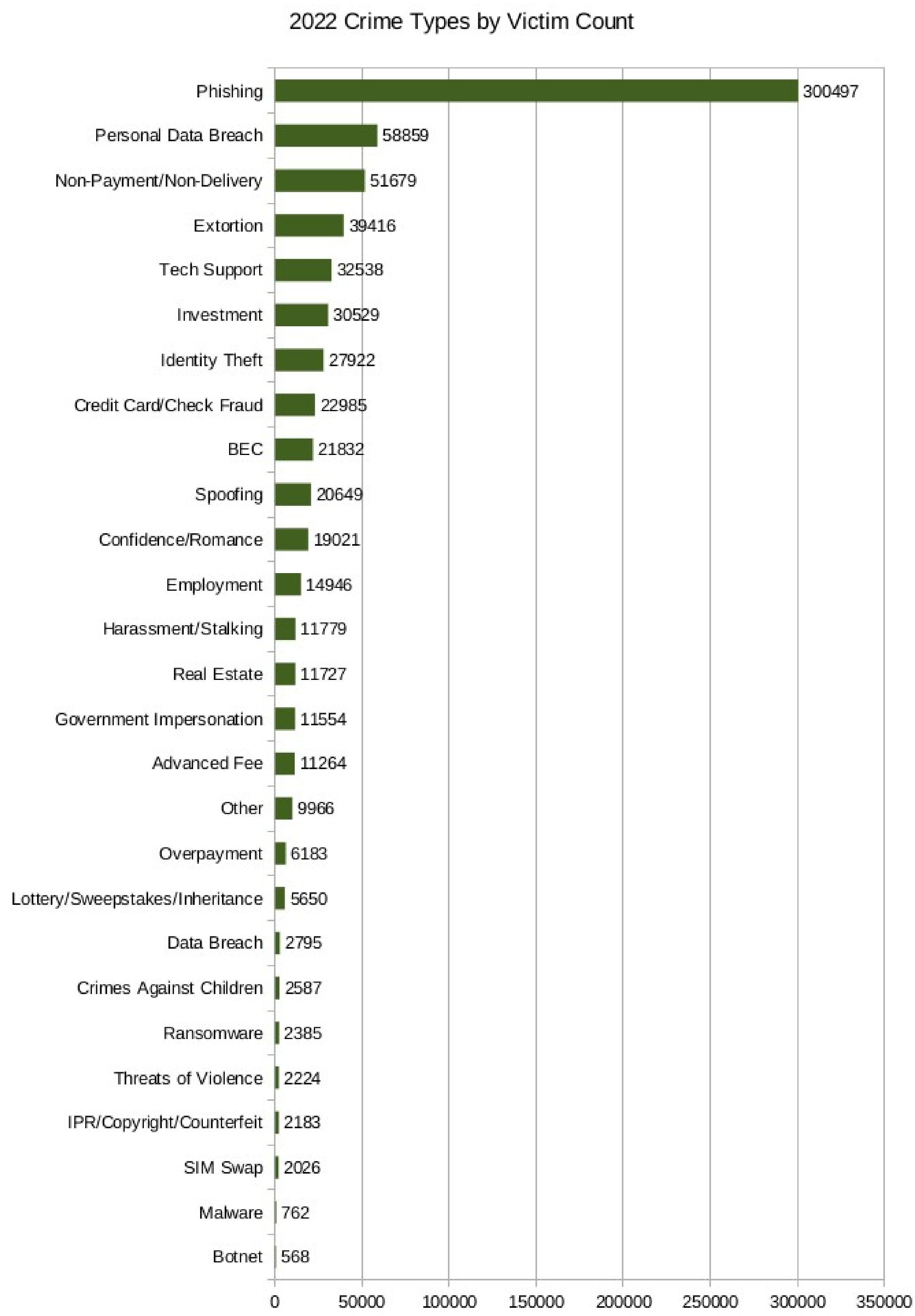

Figure 1: 2022 IC3 Internet Crime Report

and limitations to provide an overview of and recommendations for the identification, mitigation, and prevention of SE in cyberspace.

The remainder of this report will be thus organised: *Section 2* will focus on SE definitions, categories, and actors, as well as prevention and mitigation techniques. *Section 3* will discuss US law and attribution statutes, with a particular focus on investigative methods, transnational attribution, and prosecution bodies, foci, and limitations based on historical precedent. *Section 4* will provide report conclusions and recommendations.

2. Social Engineering in Perspective

2.1 Definition and Characterisation

SE is defined as "the art of influencing individuals in order to gain confidential information such as passwords, addresses, bank details, etc. by exploiting human vulnerabilities" (Alami et al., 2021: 657). It takes a number of forms with different technological requirements (Table 1; Alami et al.,2021; Safi & Singh, 2023) and varying motivations (Table 2; Chawla et al., 2023; Safi & Singh, 2023). Depending on the goals of the actor and the vulnerabilities of the target, an SE attack can use multiple vectors and have multiple objectives (Bullée & Junger, 2020). A stronger conviction of the latter may determine the sophistication of the former, so it is important to establish the relationship between them for prevention and mitigation.

Table 1: SE Attack Vectors

SE Attack	Characteristics	Subsequent Crimes
Phishing	Often an "email with a harmful attachment [or] links to fake websites that are created to steal your personal information" (CISA, 2018)	Data breach, BEC, banking fraud, ATP, malware, identity theft, extortion
Baiting	Often a media artifact of some kind, "a music or movie download [or] a USB flash drive" (Azhar et	Malware, ATP, extortion, ransomware

	al., 2023: 15) with a malicious execution embedded.	
Tailgating	"The act of following an authorised person into a restricted area or system" (Andrii et al., 2021: 485)	Corporate espionage, data breach, malware
Quid Pro Quo	Usually "scammers who pretend to be tech support" (Ali et al., 2023: 0496) offering a service which requires a malicious download	Credit card fraud, advanced fee, identity theft, non-payment/non-delivery
Vishing	"Voice phishing" (Armstrong et al., 2020: 315); persuasion techniques by phone to gain sensitive or personal information.	Identity theft, credit card fraud, non-payment/non-delivery
Pretexting	Often a prelude to phishing; uses "pre-designed scenarios" (Girinoto et al., 2022) based on research to put targets at ease and gain their trust.	Data breach, corporate espionage, extortion
Website spoofing	"An illegal website that masquerades as a legitimate one" (Alasmari et al., 2023: 1) to procure sensitive or personal data.	Data breach, fraud, identity theft
Face-to-face	Often utlised to acquire keys or other artifacts to facilitate a larger attack (Bullée & Junger, 2020).	Corporate espionage, data breach, identity theft

Table 2: SE Motivation

Objective	**Attack Characteristics**
Financial gains	Requires access to banking app login credentials; comprises the majority of phishing attacks
Defamation	Requires social media access; done with the intention of embarrassing/humiliating the victim
Impersonation	Actors mimic the identity of a third party to engage in malicious behaviour; can have financial, fraud, or defamatory motives
Identity fraud	Huge demand on the Darkweb; phishers can sell harvested credentials to bad actors. Very difficult to track and prevent.
Espionage	Corporate espionage involves stealing trade secrets; state espionage often involves malware dissemination and APT attacks
Malware Installation	Email is a popular form of dissemination. Used for espionage, ransoming and encryption, and backdoor installation

A “recent meta-analysis of 48 field experiments” (Steinmetz, 2023: 246) found a weighted rate of success among SE attacks to be 21%. This rate is due in great part to the simplicity and reproducibility of the SE attack life-cycle (Figure 2; Ali et al., 2023).

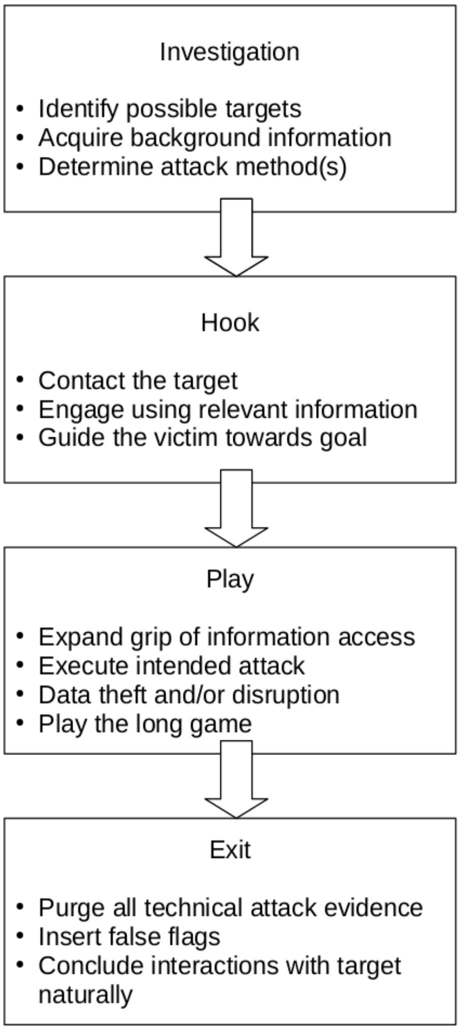

Figure 2: SE Attack Life-cycle

SE success depends on the trust inherent in social interactions (Ali et al., 2023; Bullée & Junger, 2020). The SE attack life-cycle is designed to streamline the establishment of this through the *Investigation* and *Hook* phases. Additionally, the scope of target identification need not be limited to a specific individual (though more skilled actors often practice this, called *spear phishing* (Pahi & Skopik, 2020). If an exploitation profile for a vulnerable group is compiled, then spam emails or spoofed websites tailored to lure this type of target can be deployed *en masse* without much extra effort by the malicious actor.

2.2 Actors and Targets

While the SE attack life-cycle provides streamlined entry into malicious interactions, the motivations of the actors and the vulnerabilities of the targets also play a crucial role in attack success. Understanding the characteristics of actors (Table 3; Gupta et al., 2024; Bateman, 2022) and how these influence the targets they choose (Table 4) are critical to determining proper prevention and mitigation tactics and frameworks. It is said of SE that the best technical security in the world is powerless against a vulnerable employee (Alami et al., 2021).

Table 3: SE Actor Classification

Classification	Actor Characteristics
Beginners	Those just learning cyber security/social engineering practices.
Spying Squad	Those who target specific users to spy on without ulterior motives.
Fraudsters	Those who intend to commit fraud by stealing credentials through phishing.
Enviers	Those who wish to defame or embarrass a target due to emotional factors.
Government Agencies	Often in the form of spear phishing, these attacks are carried out for a variety of reasons. Is often the first phase of a larger attack.
Miscellaneous Entities	Can be hired by a government agency, or may have political or economic motives. Is often the first phase of a larger attack.

Table 4: SE Target Classification

Classification	Possible Actors	Notable Attack(s)	Attack Motivation
Individual target	Beginners, fraudsters, spying squad, enviers	Phish Phry (Muntode & Parwe, 2019	Gain account numbers and passwords
Corporate target	Fraudsters, government agencies, misc. entities	Phishing attack on Twitter (Mackleprang & Witman, 2022); RSA Security (Parmar, 2012)	Financial fraud, identity theft, money laundering; Employee credentials, data theft, backdoor installation
Financial target	Fraudsters, misc. entities	bZx crypto heist (Yachyn, 2022)	Financial fraud, BEC
Government target	Government agencies, misc. entities	Attack on DHS (Chua, 2021)	Data theft (personal health records)

Target vulnerability stems from the interaction between their individual temperament and the persuasion skill set employed by the actor. Authority, commitment, distraction, "liking, similarity, and deception" (Armstrong et al., 2020) are all tactics actors use to inspire a psychological reaction, such as social compliance, social proof (herd mentality), and visceral triggers (need and greed) (Armstrong et al., 2020; Stajano & Wilson, 2011), to give the actor what they want. Targets of SE risk economic, data, and reputation loss in the event of a successful attack (Cross & Gillett, 2020). As will be discussed below, this makes the human element of cybersecurity extremely important, as it can easily circumvent technological security protocols protecting the targeted system from malicious action.

Additionally, state and non-state international actors may choose to target the US because (1) US internet architecture is among the most developed globally (U.S. News, 2024) and provides the largest and most complex attack surface, (2) the US has robust financial institutions and is the leading developer of blockchain technology (Aisenman, 2022; Sharma, 2023), inviting fraud, and (3) the US government and/or economy is in opposition to the actors' own political or economic cause and is thus considered an enemy. Russia, China, Iran, and North Korea state and non-state actors currently have the highest rates of US cybercrime attribution for these reasons (Machtiger, 2021; Yadav, 2024).

2.3 Prevention and Mitigation

There are several strategies organisations and institutions can provide to prevent or mitigate an SE attack. Farooq et al. (2023) have compiled an exhaustive classification list in their systematic literature review on the subject (Figure 3). While heuristic (Random Forest Classifier, 99.57% accuracy (Gupta et al., 2021)), visual similarity (Fuzzy Set Technique, 99.77% accuracy (Hidayat et al., 2021)), list based technique (PART algorithm, 99.33% accuracy (Barraclough et al., 2021)), machine learning techniques (Random Forest algorithm, 99.33% accuracy (Stobbs et al., 2020)), and deep learning techniques (CNN, 99.98% accuracy (Wei et al., 2020)) all perform well in laboratory settings, the continued high rate of successful SE attempts (FBI, 2022) belies their prevention limitations in the wild.

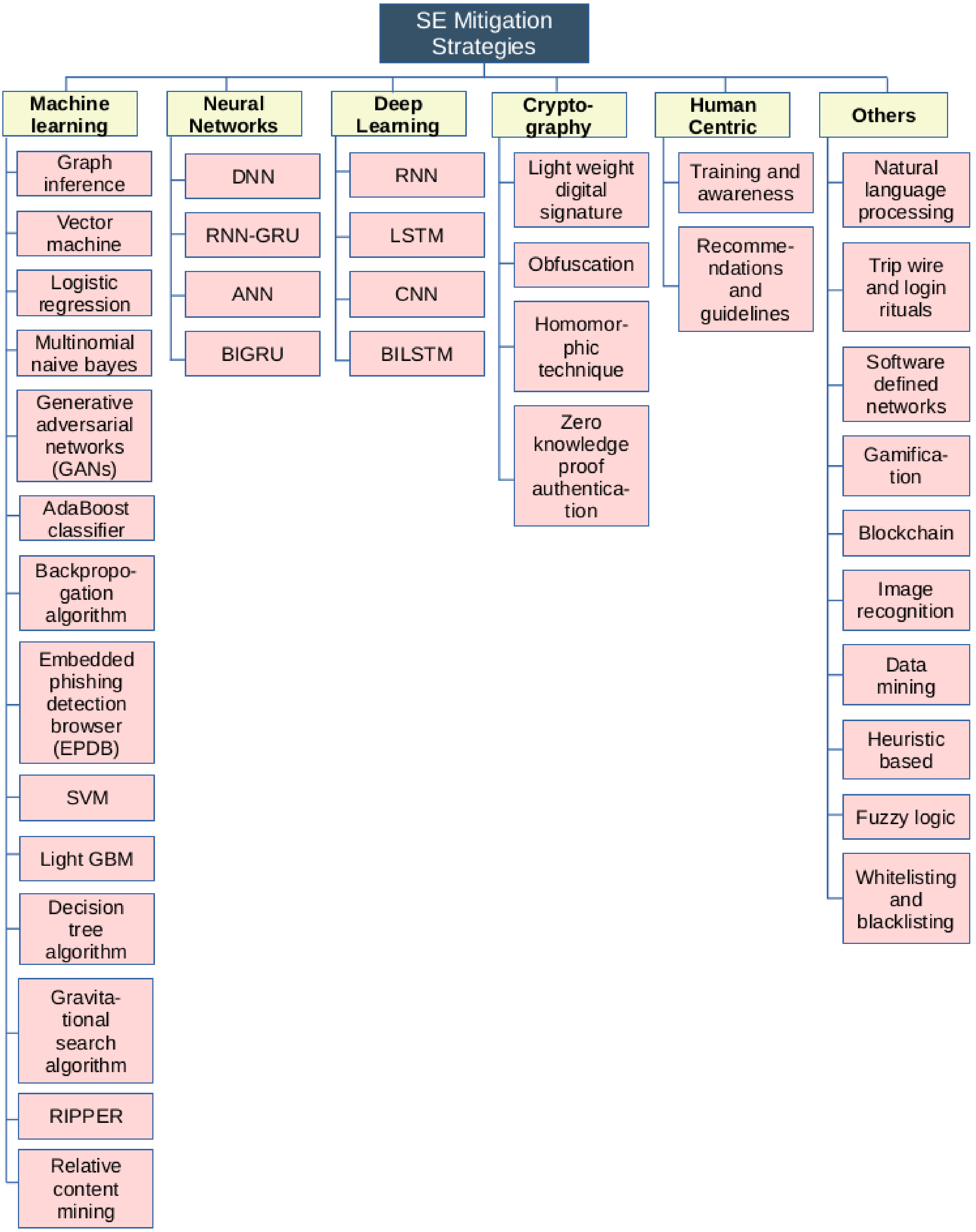

Figure 3: Categorised SE Mitigation Strategies

These performance discrepancies are due to the unpredictable nature of real-world SE attacks. Artificial intelligence systems require training sets and models to perform accordingly, which cannot be replicated outside the laboratory setting (Benevenuto et al., 2019). Thus it can be concluded that, while these tactics are indeed useful and worthy of development, they will not provide comprehensive SE prevention alone.

The human element also plays a role in technology's preventative limitations. Individuals are notoriously unpredictable preventative agents due mainly to the psychological vulnerabilities discussed in Section 2.2. There is also the issue of security fatigue, whereby instituted preventative measures are perceived as an obstacle or hassle to those they are meant to help and are ignored, thus nullifying any intended benefits (Farooq et al.,2023). In addition, while SE prevention training and education are cited as essential to organisational and individual cybersecurity (Cross & Gillett, 2020; Farooq et al., 2023), studies show mixed results of success (Cross & Gillett, 2020). Indeed, one study by Junger et al. (2017) found that providing warnings to subjects actually *increased* their rate of disclosure.

Though the data could be discouraging, education and training is nevertheless cited as an indispensable SE mitigation element (Ali et al., 2023; Alkhalil et al., 2021; Azhar et al., 2023; Farooq et al., 2023), even if it cannot completely prevent SE attacks. That said, it can be inferred that there is no comprehensive strategy which can completely prevent SE attacks, which means larger attacks are currently inevitable.

2.3.1 Artificial Intelligence

It should be noted that NLP chatbots are being utilised by actors to scale up SE attack production (Abiodun et al., 2024; Yadav, 2024). This increase in scope and scale of attack "turns old widom in cybersecurity [...] on its head” (Yadav, 2024: 11). While this area of SE research is nascent, it may prove current SE prevention methods less effective than they are reported currently.

3. Investigation, Attribution, and Prosecution

The US leads the world in attribution and prosecution of cybercrime (Bateman, 2022; Chuanying & Perkovich, 2022; Machtiger, 2021). Investigation is undertaken by joint task forces run by the FBI, DOJ, USSS, and DHS (Jimoh, 2023; Machtiger, 2021). Additionally, attribution is also reported by private technology and cybersecurity companies (Jimoh, 2023). Though the lack of a central investigative body and the proliferation of private attribution reports (Bateman, 2022) have been criticised for disorganisation and sub-standard evidence, respectively, it is this report’s position that these are unfounded.

Firstly, while task forces are under the provision of different government departments, they follow the same investigative standard (Figure 4; Lee & Levite, 2022) under the same legal framework, the CFAA (LLI, n.d.; Dougherty & Đurić, 2022). Additionally, most investigations are a joint effort between departments and thus amalgamate their investigative resources accordingly. Private attribution reports do often stem from secondary evidence sources (Bateman, 2022; Jimoh, 2023), but publication of these resources also provides pressure to government departments to stay abreast of cybersecurity trends to avoid embarrassment or accusations of negligence.

There are a number of investigative techniques that are possible to forensically link SE attacks to actors, including perimeter monitoring logs, social networking statistics, identities, spelling (typos in a URL), and domains and DNS, which examine artifacts to determine culpability (Pahi & Skopik,

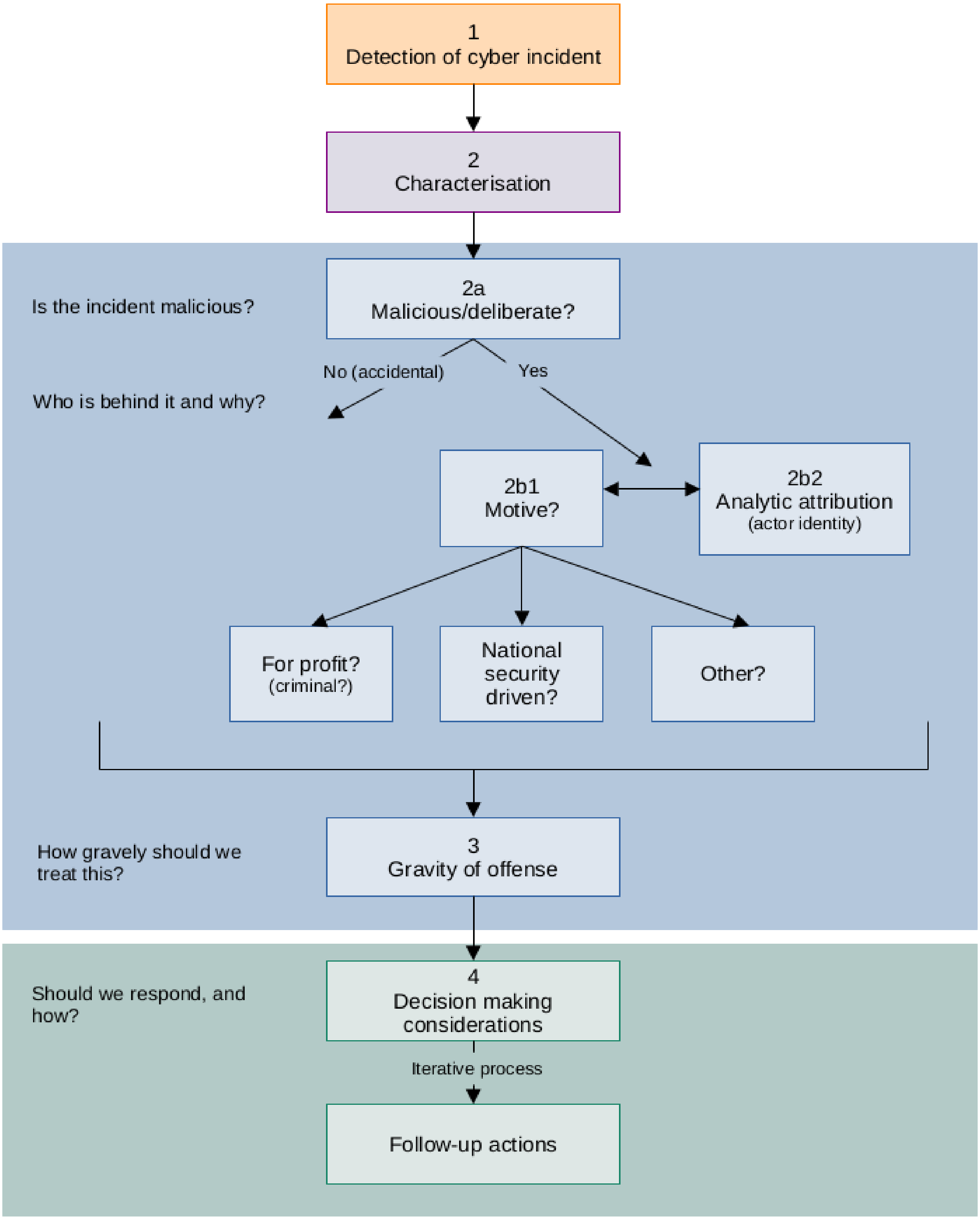

Figure 4: SE Investigative Framework

Table 5: Artifact Classification and Attribution

Attribution Type	Trustworthiness
General TTPs (typical modus operandi)	4.2 (0.7)*
Software tools frequently used	3.1 (0.5)
Phishing attempts	2.1 (0.9)
Identities, pseudonyms, and personas	3.2 (1.8)
Cloud services and C2 infrastructure used	4.6 (0.4)
DNS patterns	4.4 (0.5)
Local Malware and their properties	2.3 (1.3)
Traces in the Darknet consistent with technical artifacts	1.2 (2.1)
Encounters in the real word	3.3 (1.2)
*Numbers in brackets represent the standard deviation	

2020). Unfortunately, a study by Pahi & Skopik (2020) found the success of these forensic methods test poorly when compared to technology-focused artifacts (Table 5; SE-applicable artifacts are bold). SE-applicable artifacts averaged a trustworthiness score of 2.84 and a standard deviation of 1.3, while technology-focused artifacts averaged 3.55 with a standard deviation of 0.73. It is notable that *DNS patterns* is the highest rated SE-applicable artifact with the lowest standard deviation, as it too is technology-focused. These results may also provide an explanation for why US law does not currently favor SE attacks in attribution and prosecution, as the forensics behind them are less trustworthy.

This is particularly important in transnational cybercrime attribution and prosecution, as these scenarios are often zero-sum due to the embarrassment the accused faces if correct and the accuser faces if incorrect (Bateman, 2022; Lee & Levite, 2022). Because there is a lack of international legal consensus regarding the burden of proof for cybercrime (Collard, 2022; Jimoh, 2023; Machtiger, 2021), demonstrable investigative measures must be provided when accusing another state. Attribution is particularly beholden to this, as it is the US government's main deterrence tool for state and non-state actors (Bateman, 2022).

Concerning prosecution, *Table 6* (LLI, n.d.; Machtiger, 2021) shows a list of statutes which have been used by the DOJ to indict foreign actors for cybercrime, none of which would allow an actor to be charged with SE as the sole proof of crime. There would need to accompany another applicable crime, such as fraud, theft, or unlawful access with demonstrable losses of money, data, or trade secrets. Indeed, this lack of legal applicability of SE attacks may also contribute to its popularity as a cybercrime. Because it is more difficult to attribute and prosecute, it is allowed to proliferate. This would suggest that *de facto* methods for SE mitigation and prevention may hold more relevance than *de jure*.

Table 6: Computer Fraud and Abuse Act

Crime	**Statute**
Unlawful Computer Access	18 U.S.C. § 1030(a)(2)
Accessing a Computer to Defraud of Obtain Value	18 U.S.C. § 1030(a)(4)
Damage to a Computer	18 U.S.C. § 1030(a)(5)
Trafficking in Passwords	18 U.S.C. § 1030(a)(6)
Threatening to Damage a Computer	18 U.S.C. § 1030(a)(7)
Wire Fraud	18 U.S.C. § 1343
Bank Fraud	18 U.S.C. § 1344
Access Device Fraud	18 U.S.C. § 1029
Economic Espionage & Theft of Trade Secrets	18 U.S.C. §§ 1831, 1832
Identity Theft	18 U.S.C. §§ 1028, 1028A
Money Laundering	18 U.S.C. §§ 1956, 1957

4. Conclusions and Recommendations

This report has aimed to discuss the definition, characteristics, mitigation and prevention, and investigative, attributive, and prosecutorial aspects of social engineering as a cyber attack. Through a review of the literature, the following has been concluded:

- SE attacks utilise persuasion tactics to influence the psychological vulnerabilities of targets to divulge information through phishing, vishing, website spoofing, baiting, and tailgating, often for economic fraud, data theft, or espionage.
- Though technological mitigation techniques are a valuable aspect of prevention, they are not full-proof. Human centric measures are thus also required for more comprehensive prevention.
- At the same time, human-centric prevention has shown mixed results of success, as individuals can experience security fatigue or retain susceptibility even after education and training.
- While there are available artifacts for digital forensic investigation, those for SE tend to be less reliable than technology-focused artifacts.
- This may contribute to the lack of focus on SE for transnational attribution and prosecution, as these require solid digital forensic evidence due to the political risk of false allegations.

With these findings in mind, the following policy recommendations are made:

- Foci for individuals in organisations and government should be on education and training with strong security protocols to follow.
- At the same time, use of mitigative technologies should be encouraged in tandem with human centric prevention with the knowledge that an eventual breach is likely, and should therefore be monitored through log assessment and other forms of preventative measures.

- Though SE as a standalone crime is usually not sufficient for attribution or prosecution under current international and US law, SE attacks used in conjunction with larger attacks should be given more weight during the attribution and/or prosecution processes. This would raise public awareness and may also act as a deterrent to state and non-state actors.

5. References

Abiodun, M. et al. (2024) Unveiling the Dark Side of ChatGPT: Exploring Cyberattacks and Enhacing User Awareness. *Information*, 15 (27): 1 – 26

Aisenman, J., Ito, H., Pasricha, G. K. (2021) Central Bank Swap Arrangements in the Covid-19 Crisis. *Journal of International Money and Finance*, 122: 1 – 20

Alami, A. O. et al. (2021) Overview of Social Engineering Attacks on Social Media. *Procedia Computer Science*, 198: 656 – 661

Alasmari, N. et al. (2023) Metaheuristics with Deep Learning Driven Phishing Detection for Sustainable and Secure Environment. *Sustainable Energy Technologies and Assessments*, 56: 1 – 7

Ali, M. L. et al. (2023) Social Engineering Incidents and Preventions. *In: IEEE 13th Annual Computing and Communication Workshop and Conference (CCWC)*. IEEE: 0494 – 0498

Andrii, Y, et al. (2021) Social Engineering in the Context of Cybersecurity. In: *Interaction of Society and Science: Problems and Prospects: Abrstracts of XXX International Scientific and Practical Conference.* London, England: 484 – 488

Armstrong, M. E. et al. (2021) How Social Engineers Use Persuasion Principles During Vishing Attacks. *Information & Computer Security*, 29 (2): 314 – 331

Azhar, M. B. M. et al. (2023) Social Engineering and Cyber Threats: Exploring Techniques, Impacts, and Strategies. *International Journal of Accounting*, *Finance*, *and Business*, 8 (50): 13 – 25

Barraclough, P.A., Fehringer, G., Woodward, J. (2021) Intelligent Cyber-phishing Detection for Online. *Computer & Security*, 104: 1 – 17

Bateman, J. (2022) The Purpose of U.S. Government Public Cyber Attribution: A Legal Perspective. In: Chuanying, L. et al. (eds.) *Managing U.S.-China Tensions Over Public Cyber Attribution*. Carnegie Endowment for International Peace: 14 – 24

Benevenuto, F., Correia, A., Murai, F., Reis, J. C. S., & Veloso, A. (2019) Explainable Machine Learning for Fake News Detection. In: WebSci '19, 30 June – 3 July, 2019, Boston, MA, USA. ACM: 17 – 26

Bullée, J-W. & Junger, M. (2020) Social Engineering. In: Holt, T.J. & Bossler, A. M. (eds.) *The Palmgrave Handbook of International Cybercrime and Cyberdeviance.* Palmgrave: 849 – 875

CISA (2023) *Recognize and Report Phishing* | Secure Our World. cisa.gov [Available online] https://www.cisa.gov/secure-our-world/recognize-and-report-phishing

Chawla, M., Goenka, R., & Tiwari, N. (2023) A Comprehensive Survey of Phishing: Mediums, Intended Targets, Attack and Defence Techniques and a Novel Taxonomy. *International Journal of Information Security*: 1 – 30

Chua, J. A. (2021) *Cybersecurity in the Healthcare Industry: It Pays to be Vigilant Against Political Attacks*| Cyber Security. Podiatry Management: 69 – 72

Chuanying, L. & Perkovich, G. (2022) Conclusions and Recommendations. In: Chuanying, L. et al. (eds.) *Managing U.S.-China Tensions Over Public Cyber Attribution*. Carnegie Endowment for International Peace: 49 – 55

Collard, S. (2022) Cyber Attribution Lessons from the Maritime Domain. In: Chuanying, L. et al. (eds.) *Managing U.S.-China Tensions Over Public Cyber Attribution*. Carnegie Endowment for International Peace: 1–5

Cross, C. & Gillett, R. (2020) Exploiting Trust for Financial Gain: An Overview of Business Email Compromise (BEC) Fraud. *Journal of Financial Crime*, 27 (3): 871 – 884

Đurić, N. L. & Dougherty, T. (2022) The United States Approach to the Investigation and Prosecution of Cybercrime and Cryptocurrency Crime. Hrvatski ljetopis za kaznene znanosti i praksu, 29 (2): 409 – 431

Farooq, A. et al. (2023) Mitigation Strategies Against the Phishing Attacks: A Systematic Literature Review. *Computers & Security*, 132: 1 – 25

FBI (2022) Internet Crime Report 2022. *The Internet Crime Complaint Center* (IC3). FBI: 2 – 32 **[Available Online] https://www.ic3.gov/Media/PDF/AnnualReport/2022_IC3Report.pdf**

Girinoto et al. (2022) OmeTV Pretexting Phishing Attacks: A Case Study of Social Engineering. *In:* 7*th* *International Workshop on Big Data and Information Security*. IEEE: 119 – 124

Gupta, B. B. et al. (2021) A Novel Approach for Phishing URLs Detection using Lexical Based machine Learning in a Real-time Environment. *Computer Communications*, 175: 11 – 57

Gupta C. et al. (2024) Anti-Phishing: A Comprehensive Perspective. *Expert Systems with Applications*, 238: 1 – 34

Hidayat, R. et al. (2021) Similarity Measure Fuzzy Soft Set for Phishing Detection. *International Journal of Advances in Intelligent Infomatics*, 7 (1): 101 – 111

Jimoh, M. (2023) Critiquing the U.S. Characterization, Attribution and Retaliation Laws and Policies for Cyberattacks. *Computer Law & Security Review*, 50: 1 – 12

Junger, M., Montoya, L., & Overink, F-J. (2017) Prining and Warnings are Not Effective to Prevent Social Engineering Attacks. *Computers in Human Behavior* (66): 75 – 87

Lee, J. & Levite, A. E. (2022) Attribution and Characterization of Cyber Attacks. In: Chuanying, L. et al. (eds.) *Managing U.S.-China Tensions Over Public Cyber Attribution*. Carnegie Endowment for International Peace: 33 – 42

LLI (n.d.) *18 U.S. Code ss 1030 – Fraud and Related Activity in Connection with Computers* | Legal Information Institute. Cornell Law School. [Available Online] https://www.law.cornell.edu/uscode/text/18/1030

Machtiger, P. G. (2021) Deconstructing the U.S. Policy of Indicting Malicious State Cyber Actors. *New York Journal of Legislation and Public Policy*, 24 (1): 253 – 312

Mackleprang, S. & Witman, P. D. (2022) The 2020 Twitter Hack – So Many Lessons to be Learned. *Journal of Cybersecurity, Education, Research and Practice*, 2021 (2): 1 – 11

Muntode, A. R. & Parew, S. S. (2019) An Overview on Phishing – Its Types and Countermeasures. *International Journal of Engineering Research & Technology*, 8 (12): 545 – 548

Pahi, T. & Skopik, F. (2020) Under False Flag: Using Technical Artifacts for Cyber Attack Attribution. *Springer Open*, 3 (8): 1 – 20

Parmar, B. (2012) Protecting Against Spear-phishing. *Computer Fraud & Security:* 8 – 11
Safi, A. & Singh, S. (2023) A Systematic Literature Review on Phishing Website Detection Techniques. *Journal of King Saud University – Computer and Information Sciences*, 35: 590 – 611

Sharma, T. K. (2023) *Top 10 Countries Leading Blockchain Technology in the World* | Blockchain Council. blockchain-council.org. [Available online] https://www.blockchain-council.org/blockchain/top-10-countries-leading-blockchain-technology-in-the-world/

Stajano, F. & Wilson, P. (2011) Understanding Scam Victims: Seven Principles for Systems Security. *Communications of the ACM*, 54 (3): 70 – 75

Steinmetz, K. F. (2023) Executing Effective Social Engineering Penetration Tests: A Qualitative Analysis. *Journal of Applied Security Research*, 18 (2): 246 – 266

Stobbs, J., Issac, B., & Jacob, S. M. (2020) Phishing Web page Detection using Optimised Machine Learning. *In: IEEE 19th International Conference on Trust, Security, and Privacy in Computing and Communications*. IEEE: 483 – 490

U.S. News (2024) *These Countries Have the Most Well-Developed Digital Infrastructure* | Best Countries. usnews.com [Available online] https://www.usnews.com/news/best-countries/rankings/well-developed-digital-infrastructure

Wei, W. et al. (2020) Accurate and Fast URL Phishing Detector: A Convolutional Neural Network Approach. *Computer Networks*, 178: 1 – 9

Yachyn, O. (2022) Consequences of Using Centralisations in Blockchain Applications. Masters thesis.

Yadav, S. (2024) Social Automation and APT Attributions in National Cybersecurity. *Journal of Cyber Security Technology:* 1 – 26