BULLETIN
OF "CAROL I" NATIONAL DEFENCE UNIVERSITY

https://buletinul.unap.ro/index.php/en/

Shielding Against Social Engineering Threats: A Counterintelligence Approach

Anastasios-Nikolaos KANELLOPOULOS, PhD Candidate*

*Department of Business Administration, Athens University of Economics and Business, Greece
e-mail: ankanell@aueb.gr

Abstract

In an increasingly networked global context, commercial counterintelligence units and competitive intelligence experts must deal with sophisticated social engineering threats that exploit human psychology rather than technological shortcomings. This article highlights the importance of counterintelligence training and robust security measures while analyzing the psychological manipulation tactics employed by adversaries to lower these risks.

The article examines social engineering strategies such as scarcity, authority, reciprocity, fear, and trust qualitatively to emphasize the significance of behavioral defenses and organizational awareness. The methodology, which evaluates institutional responses and psychological exploitation strategies, incorporates a review of the literature and expert comments. The paper's conclusion recommends a multi-layered approach that incorporates organizational cultural reforms, technical defenses, and psychological awareness to safeguard sensitive data from insider threats and social engineering.

Keywords:

Social Engineering; Counterintelligence; Human Psychology; Insider Threats; Security Awareness.

Article info

Received: 14 July 2025; Revised: 19 August 2025; Accepted: 15 September 2025; Available online: 6 October 2025

Citation: Kanellopoulos, A.N. 2025. ”Shielding Against Social Engineering Threats: A Counterintelligence Approach.” *Bulletin of ”Carol I” National Defence University*, 14(3): 245-259. https://doi.org/10.53477/2284-9378-25-46

In today's intelligence environment, competitive intelligence has evolved from a reactive, market-focused discipline to a proactive function that shields companies from espionage, cyberthreats, and insider threats. In industries where economic competition and geopolitical conflicts collide, such as shipping, energy, and key infrastructure, the human element has become the most vulnerable entry point for adversaries. Conventional cyber defenses focus on technical safeguards, but in order to circumvent these barriers, adversaries are increasingly employing social engineering—the art of playing on people's emotions to get personal information or gain illegal access. This kind of attack is a significant problem for companies that have not adequately addressed the human dynamics that underlie their security architecture.

Social engineering attacks are effective because they exploit predictable psychological trends. Adversaries impersonate authority figures, exploit emotions like fear and trust, and generate urgency through scarcity. Additionally, they exploit the reciprocal social norm. By doing this, they circumvent rational barriers and trigger instinctive human responses that lead to the disclosure of personal information or the commission of criminal activity. Organizations that do not understand these psychological methods remain vulnerable, regardless of how advanced their technology is.

This article explores the connection between counterintelligence tactics, human psychology, and social engineering within the context of competitive intelligence. The primary objectives are to analyze how adversaries exploit psychological triggers and propose responses that combine technical controls with human awareness. The article uses a qualitative methodology and incorporates insights from the intelligence community, industry best practices, and academic literature.

The article also argues that a multipronged approach is required to counteract social engineering. Training and awareness efforts must first educate staff members about the psychological manipulation techniques employed by enemies. Second, human attention to detail must be used to supplement technical defenses with robust security measures, including encryption, anomaly detection systems, and extensive access controls. Third, systems that identify insider threats must monitor for any anomalous activity that could indicate an internal breach. Together, these protections offer a robust defense against human-centered attacks.

In the next chapters, the paper offers practical strategies for safeguarding sensitive data while also analyzing the evolving danger landscape of social engineering and breaking down the psychological concepts employed by adversaries. Through this complete analysis, the article highlights the value of counterintelligence training and a security-conscious company culture in mitigating human vulnerabilities, which remain the weakest link in the intelligence security chain.

The Intersection of Counterintelligence and Social Engineering

The Critical Importance of Counterintelligence

Counterintelligence (CI) is a crucial component of national security because it safeguards the sanctity of classified information, prevents foreign enemies from scheming, and maintains the integrity of national secrets (Shulsky and Schmitt 2009; Foryst 2010; Kanellopoulos 2024a). In an era of unprecedented global interconnectedness, where digital espionage and manipulation have become pervasive threats, social engineering has emerged as a significant challenge in the field of CI, which faces a constantly changing and complex landscape (Sims and Gerber 2009; Kuloğlu, Gül and Erçetin 2014; Barnea 2019). At its core, CI encompasses both offensive and defensive strategies, with counterespionage being a crucial component of the former. Understanding the intricate role of CI requires a further investigation of these components (Prunckun 2019; Kanellopoulos 2022).

Offensive CI is the proactive and strategic component of CI that focuses on identifying and removing threats from foreign intelligence agencies (FIS) and hostile organizations. The primary objective of offensive CI is to stop espionage activities that can endanger national security (Moyers 2025). This means learning the strategies and tactics that adversaries employ and using this knowledge to thwart their efforts. One essential element of offensive CI is counterespionage. Counterespionage, which includes a wide range of activities, is frequently seen as the first line of defense against spies. This means conducting operations to track down foreign operatives, keeping tabs on their movements, and learning about the methods and techniques used by enemy intelligence services. Double-agent operations, which involve convincing a foreign spy to join the host country's intelligence service, are another tactic offensive counterintelligence agents may use to turn the tables on the enemy (Stouder and Gallagher 2013).

Additionally, defensive CI strengthens the offensive components by focusing on preventing illegal access and exfiltration of sensitive information and classified data (Johnson 2010). It entails proactively and thoroughly identifying the national security apparatus's flaws (Sithole and Du Toit 2022). Defensive CI includes digital and physical security measures as well as personnel security protocols. In the subject of defensive CI, countermeasures against social engineering are essential. Salama and Fadi Al-Turjman (2023) define social engineering as the act of deceiving someone into divulging personal information or permitting unauthorized access. It frequently involves psychological manipulation, deception, and the exploitation of human emotions such as trust and fear. Because social engineering can occur both in person and online, it is a challenging problem in this age of advanced technology (Reynolds 2016; Hatfield 2018). In the modern era, the line between physical and digital security has blurred, and CI needs to adapt to a changing and connected landscape. The ability to anticipate and respond to foreign opponents' evolving tactics is essential. In addition to a commitment to safeguarding national secrets, this necessitates a blend of technology expertise, strategic planning, and human intelligence (Reynolds 2016).

Social Engineering as a Gateway

A significant risk to national security, social engineering is a strong and secretive technique that has emerged as a key entrance point for espionage operations. Adversaries that are adept in psychological manipulation and dishonest techniques employ this tactic to get illegal access to sensitive information, exploit vulnerabilities, and eventually endanger a nation's security (Breda, Barbosa and Morais 2017). These sophisticated attacks typically target specific persons within an organization since humans are typically regarded as the weakest link in the security chain. At its fundamental level, social engineering is a form of manipulation that relies on human psychology and trust (Reynolds 2016; Hadnagy 2018). It can take many different forms and be done both in the actual and digital worlds. Influencing people to reveal personal information or perform actions they wouldn't often consider taking is the primary goal of social engineering assaults. Cybercriminals can obtain illegal access to computer systems and sensitive data by revealing passwords, allowing access to secure areas, or clicking on harmful links in emails (Hatfield 2018; Syafitri, et al. 2022).

Furthermore, social engineers are skilled at exploiting traits and tendencies that are common to all people, such as curiosity, trust, fear, and the desire to be helpful (Reynolds 2016; Hadnagy 2018). They can pose as trustworthy colleagues, IT support personnel, or even superiors like auditors or police enforcement. By employing these personas to build rapport and trust, they can more readily persuade their targets to violate security protocols (Matyokurehwa, et al. 2022). The social engineering method known as "phishing" is widely used. Phishing attempts often use convincingly fake emails that look real. These emails persuade recipients to give personal information, download dangerous files, or click on links that lead to malicious websites. Such assaults can have catastrophic consequences since they have the potential to undermine whole networks and the integrity of a nation's sensitive data (Bhavsar, Kadlak and Sharma 2018).

Eventually, social engineering is particularly harmful because it does not call for sophisticated hacking tools or technological know-how (Gray 2021). Instead, it makes use of human nature and the inclination for people to believe in and assist others. This makes it challenging to fight against, as traditional cybersecurity technologies like firewalls and antivirus software often fail to stop these attacks. In each organization's security chain, people are typically the weakest link (Reynolds 2016; Hadnagy 2018).

The Anatomy of Social Engineering Attacks

The Spectrum of Social Engineering Attacks

Adversaries now employ a wide variety of effective strategies, including social engineering assaults, to trick people into inadvertently exposing personal information and jeopardizing security (Erbschloe 2020). These approaches, which exploit human psychology, trust, and vulnerabilities, are typical of a range of strategies used by adversaries in the digital age (Reynolds 2016; Hadnagy 2018). It is necessary to comprehend this spectrum in order to strengthen defenses against these cunning attacks.

Phishing is a prevalent social engineering tactic whereby thieves send phony emails or messages purporting to be banks or reputable companies in an attempt to steal private information, such as financial information or passwords (Bhavsar 2018). By creating a sense of urgency or panic, such as notifications about hacked accounts or past-due payments, these attacks usually use psychological pressure to cause victims to act rashly (Wang and Lutchkus 2023). Phishing typically involves harmful links or attachments that direct users to fake websites that appear real in order to gain login credentials or personal information (Sharma, Dash and Ansari 2022). Once they have access, hackers may commit fraud, identity theft, or other cyberattacks. For victims, money losses, data breaches, and reputational harm are serious consequences.

Furthermore, impersonation is a social engineering strategy whereby attackers pose as trustworthy individuals or organizations in order to exploit people's confidence, according to Algarni et al. (2013). In order to fool victims into responding with bogus demands, attackers pose as trustworthy companies, family members, or coworkers (Reynolds 2016; Almomani and Alauthman 2025). Attackers may use organizational hierarchy and trust to pretend to be superiors or coworkers in the workplace and request private information, like login passwords or financial information, over the phone or by email. Similarly, family-friend impersonators use emotional attachments and often fabricate crises to pressure victims into divulging personal information (Jakobsson 2018). Impersonation can also target customers through honey emails, websites, or phone calls from tech companies, banks, or government agencies. By employing compelling language, realistic logos, and stolen personal information, attackers establish urgency and believability, which prompts victims to take immediate action. Successful impersonation requires establishing confidence and capitalizing on the victim's innate desire to cooperate or assist.

Subsequently, in elicitation, attackers might utilize a subtle social engineering approach called elicitation to get sensitive information through casual conversation, as an alternative to overt tactics like phishing or impersonation (Cooke 1994). It exploits people's natural inclination toward open communication and trust (Beckers and Pape 2016). As they appear kind and unthreatening, attackers often initiate harmless talks in social or professional settings and then gradually steer the conversation toward their target information (Beckers, et al. 2017). Leading inquiries, active listening, and reciprocal sharing are some of the tactics they use to encourage disclosure and build trust. Elicitation is especially effective in situations where informal trust develops, such as social events, networking groups, or professional settings where individuals may share project, commercial, or private information without fully comprehending the hazards (Tiwari and Rathore 2017).

In addition, pretexting is the act of creating fake situations or events to pressure someone into sharing personal information. The attackers fabricate a story that sounds plausible by using a pretext that appeals to the target's emotions or aspirations. This could entail posing as a financial institution conducting a major audit or a colleague in need of assistance. These made-up scenarios compel people to reveal personal information or take actions that compromise their security (Alazri 2015).

Finally, tailgating is a physical social engineering approach that allows attackers to access secure facilities without authorization by exploiting human kindness or negligence (Sobur, et al. 2024). Unlike digital attacks, it circumvents security mechanisms by using human behavior and physical presence. When following an authorized individual via a secure entry, the attacker frequently blends in by dressing appropriately or carrying materials that appear professional in order to allay suspicions (Cheh et al. 2019). Because they think anyone in the area should be there, victims may leave the door open without verifying credentials out of courtesy or to avoid confrontation. Tailgating is prevalent in safe establishments, such as offices, where people are rushing or willing to assist. One of the risks of a successful attack is unauthorized access to sensitive areas, which could lead to data breaches or other security issues.

Exploiting Human Psychology

In the discipline of CI, understanding the psychology of social engineering is essential. A wide range of psychological ideas is commonly employed by skilled manipulators to execute their covert operations. Understanding these psychological techniques is necessary to develop effective defenses against social engineering threats (Schaab, Beckers and Pape 2017).

One of the core psychological ideas used by social engineers is authority. Adversaries typically assume the identities of authoritative individuals, such as law enforcement, senior executives, or trustworthy supervisors, in order to pressure others into meeting their demands. People's natural inclination to defer to and obey those in power can be leveraged to promote cooperation and the sharing of personal information. Because it may overcome skepticism and critical thinking simply by existing, perceived authority is a potent tool in the social engineer's toolkit (Bullée, et al. 2017).

Reciprocity is another psychological idea that enemies exploit. People frequently feel obliged to repay others when they get something beneficial or a favor. Social engineers exploit this tendency to persuade others by presenting what seems to be a benefit. Giving creates a sense of duty in the recipient, which frequently results in them returning the favor by granting access or disclosing personal information. This is true whether the present is little, a gesture of appreciation, or an informational nugget. This approach takes advantage of people's innate desire to maintain fair and balanced social relationships (Bullée, et al. 2015).

In addition, instilling a sense of urgency or scarcity is another psychological tactic social engineers employ to suppress reason. When people think a resource or opportunity is limited or in great demand, they are more likely to act impulsively. Adversaries use this sense of urgency by imposing false restrictions or time constraints on their targets. For example, they could pose as a trustworthy source and threaten to delete the user's account if they do not provide information immediately. Fear of losing out or the potential consequences of delay might cause people to act hastily, ignoring their usual caution and skepticism (Siddiqi, Pak and Siddiqi 2022).

The delicate interplay between trust and fear is a psychological tactic that adversaries utilize to obtain personal information. By inciting fear, usually through threats or terrifying scenarios, social engineers can make people feel more pressured and nervous. In this state, they are more inclined to act irrationally, which may involve divulging personal information, in an attempt to reduce perceived risks. However, trust is another tool used by social engineers to build rapport and sway their victims. When people believe they are communicating with a trustworthy person or thing, their guard is down and they are more susceptible to manipulation. A fundamental human need is trust (Siddiqi, Pak and Siddiqi 2022).

Strategies to Safeguard Against Social Engineering Threats

Counterintelligence Training

Increasing their defenses against the crafty and misleading tactics of social engineering is a more crucial task for counterintelligence agencies and companies in a time when cyber threats are increasing and the area of espionage and subterfuge is continuously evolving. In this ongoing battle, training and awareness programs are essential because they equip employees with the knowledge and skills necessary to identify, repel, and overcome these threats (Kanellopoulos 2023).

Identifying Typical Social Engineering Strategies: One of the main tenets of CI training is to help employees recognize common social engineering strategies. Phishing, impersonation, elicitations, pretexting, and tailgating are some of the tactics used to deceive people into breaking security protocols or divulging personal information. Training programs must teach participants how to spot the warning signs of these tactics, which include suspicious emails, strange demands, or people acting differently from their typical behavior. By raising awareness of the intricate nature of social engineering, organizations can cultivate a vigilant and informed staff (Aldawood and Skinner 2018).

Performing Simulated Exercises: CI training includes both theoretical and practical application. Simulations are a great way to test how employees respond to social engineering attempts in real-world scenarios. These exercises assist firms in evaluating how well-trained and equipped their staff are by mimicking enemy tactics. By simulating phishing assaults, impersonation scenarios, and other forms of social engineering, organizations can identify areas for development, evaluate the efficacy of their defenses, and adjust their training. These exercises not only evaluate personal knowledge but also foster a culture of readiness (Banjo 2024).

Promoting a Culture of Skepticism: CI training should be used to establish a culture of skepticism among employees. The importance of verifying sensitive requests and actions cannot be overstated. People must be encouraged to seek affirmation, ask questions, and restrain their initial impulses when confronted with unfamiliar or potentially hazardous circumstances. This culture of skepticism is a basic protection against social engineering since it raises the bar for manipulation. It enables employees to act as the first line of defense against potential risks by exercising caution and critical thinking (Kanellopoulos 2022).

Educating Information Value: In order for employees to comprehend the significance of safeguarding sensitive data, they must be educated regarding the value of the data they handle. Understanding the consequences of compromised information goes beyond knowledge and fosters a sense of responsibility and commitment to national security. People who are aware of the potential consequences of data breaches are more likely to take their duties seriously and exercise caution when asked for sensitive information (Eminağaoğlu, Uçar, and Eren 2009).

Robust Security Protocols

Modern organizations seeking to protect their sensitive data and preserve the integrity of their operations must establish robust security protocols. These procedures incorporate a range of measures, from comprehensive security rules to state-of-the-art technology solutions, to mitigate the dangers associated with social engineering threats (Poehlmann 2021).

Comprehensive Security Policies and Procedures: The foundation of a strong security infrastructure is the development and application of comprehensive security policies and procedures. These documents serve as the cornerstone of an organization's security plan. They define best practices for security, provide protocols for handling sensitive data, and outline the duties and obligations of employees. Additionally, they ought to go over the dangers of social engineering tactics and provide detailed guidance on how to recognize and deal with them. An educated and informed staff is essential to these policies because it ensures that employees can recognize and stop dishonest practices (Chen, Ramamurthy and Wen 2019).

State-of-the-Art Intrusion Detection Systems and Firewalls: To improve their defenses against social engineering, organizations need to deploy state-of-the-art intrusion detection systems and firewalls. These technologies are the first line of protection against internet threats such as malware, phishing schemes, and unauthorized access attempts. Through constant network traffic scanning for anomalous activity, intrusion detection systems promptly alert security professionals to potential threats. Firewalls serve as a barrier between trusted internal networks and untrusted external networks by blocking unauthorized access and eliminating potentially dangerous material. Together, these solutions offer a proactive and reactive security posture to stop and mitigate the impact of social engineering (Anwar 2017).

Two-Factor Authentication (2FA): To enhance access control and lessen the likelihood of unwanted access to sensitive systems and data, organizations ought to require two-factor authentication (2FA). 2FA adds a layer of security by combining two different authentication methods to verify the identity of individuals seeking access. This typically involves both a user-known object (such as a password or PIN) and a user-possessed item (such as a security token or smartphone). By implementing 2FA, organizations significantly reduce the likelihood that social engineers would get access through credential theft or impersonation. Even if an attacker manages to obtain a password, they will still need the second factor to obtain access (Wang and Wang 2016).

Investment in Encryption Tools: Particularly in the event of a breach, encryption is crucial for avoiding unauthorized access to private data. When information is converted into a code that can only be decoded by those with the required encryption keys, it is said to be encrypted. This ensures that even if an attacker can access the data, it is worthless and unintelligible without the decryption key. Because encryption techniques offer an additional layer of safety and render any stolen or intercepted data incomprehensible, they are essential for both data in transit and data at rest. This safeguard is particularly important when managing classified or highly sensitive information since it stops data from being abused in the event of a social engineering assault (Volini 2021).

Insider Threat Detection

Since CI methods currently recognize that internal risks can jeopardize an organization's security, it is imperative to comprehend and identify insider threats in order to protect sensitive data. Insider risks can occur when employees, contractors, or even trusted individuals intentionally breach security by abusing their access. In many cases, social engineering approaches enable these risks. To handle this pressing challenge, organizations need to employ a range of strategies and tools to actively monitor and mitigate these risks (Kanellopoulos 2024b).

Techniques for Recognizing Odd or Suspicious Behavior: The first line of defense against insider threats is putting in place systems to spot odd or suspicious conduct among staff members. Since these systems recognize that insider threats are not necessarily the result of malicious intent, they focus on identifying deviations from normal behavior. An employee who suddenly accesses an unusual amount of data, tries to circumvent security measures, or exhibits irregular work habits, for example, may be exhibiting signs of an insider threat (Georgiadou, Mouzakitis and Askounis

2021). Behavioral analytics tools can be used to monitor user activity and spot deviations from established patterns. This allows companies to respond swiftly to unusual conduct, whether it is the product of a malicious insider or an inadvertent participant in a social engineering fraud (Cho and Lee 2016).

Employee Monitoring and Auditing Systems: To keep up their proactive approach to spotting insider threats, organizations might use employee monitoring and auditing systems. These technologies provide continuous monitoring of digital activity, including file access, system logins, and data transfers (Subhani, Khan and Zubair 2021). By collecting and examining these records, organizations can identify unusual conduct and look into it further. These devices serve as a deterrent as well as a tool for danger identification since workers are aware that their actions are being observed. Knowing that their activities are being observed deters social engineers, and malicious insiders are less likely to act covertly as a result of this monitoring (Stavrou, et al. 2014).

Extensive Background Checks and Personnel Vetting: The first line of defense against insider threats is thorough personnel vetting, which includes extensive background checks for anyone with access to sensitive information. These checks should include a detailed examination of an individual's qualifications, employment history, and criminal background, if any (Beneda and Jaros 2020). Background checks also take into account a person's financial history, connections, and contacts that could influence their loyalty or susceptibility to social engineering tactics. This comprehensive screening process is crucial for identifying any red flags or potential vulnerabilities that adversaries could take advantage of. By using background checks, organizations can lower the risk of insiders who could jeopardize their security (Alsowail and Al-Shehari 2021).

Conclusion

In a modern intelligence and security environment, social engineering is one of the most dangerous and underestimated risks that enterprises must contend with. Despite advancements in cybersecurity technologies, adversaries continue to target the human element, which is the most unpredictable and vulnerable component of any security system. This article has shown how social engineers exploit fundamental psychological ideas like authority, reciprocity, scarcity, fear, and trust to get beyond rational defenses and force people to provide personal information.

Countering these attacks requires a change in viewpoint from solely technical defenses to an integrated security approach, where CI is crucial. Training programs that educate employees about the tactics and psychological manipulation techniques used by social engineers are essential to developing an educated and resilient workforce. However, training alone is not enough. Organizations must implement a wide range of security measures as a contingency in case human attention is insufficient, including intrusion detection systems, encryption software, and strong authentication methods.

In addition, the growing danger of insider threats, whether deliberate or inadvertent, highlights the need for constant behavioral surveillance, stringent recruiting procedures, and the creation of a security-focused corporate culture. Social engineering assaults are often facilitated by insider threats, who either work directly with adversaries or inadvertently enable breaches through careless behavior.

Ultimately, to safeguard sensitive data in high-risk industries like transportation, energy, and vital infrastructure, companies must acknowledge that human psychology is both a vulnerability and a defense mechanism. By predicting how attackers exploit psychological triggers, organizations can reduce their exposure to intelligence threats and proactively protect against social engineering. The article's findings emphasize that social engineering is a basic counterintelligence problem, not just a cybersecurity one, and that it calls for an all-encompassing strategy that incorporates continuous attention to detail, technology restrictions, and training. Fundamentally, the battle against social engineering is ongoing, adaptable, and psychological. Companies that invest in understanding and addressing this issue will be better able to protect their national security interests, competitive advantage, and operational integrity in an increasingly complex intelligence environment.

References

Alazri, A. S. 2015. "The Awareness of Social Engineering in Information Revolution: Techniques and Challenges." In *2015, the 10th International Conference for Internet Technology and Secured Transactions (ICITST)*. https://doi.org/10.1109/icitst.2015.7412088.

Aldawood, H., and G. Skinner. 2018. "Educating and Raising Awareness on Cyber Security Social Engineering: A Literature Review." In *2018 IEEE International Conference on Teaching, Assessment, and Learning for Engineering (TALE)*, 62–68. https://doi.org/10.1109/tale.2018.8615162.

Algarni, A., Y. Xu, Taizan Chan, and Yu-Chu Tian. 2013. "Social Engineering in Social Networking Sites: Affect-Based Model." In *8th International Conference for Internet Technology and Secured Transactions (ICITST-2013)*. https://doi.org/10.1109/icitst.2013.6750253.

Almomani, A., and M. Alauthman. 2025. *Examining Cybersecurity Risks Produced by Generative AI*. IGI Global.

Alsowail, R. A., and T. Al-Shehari. 2021. "A Multi-Tiered Framework for Insider Threat Prevention." *Electronics* 10 (9): 1005. https://doi.org/10.3390/electronics10091005.

Anwar, S., J. Mohamad Zain, M. F. Zolkipli, Z. Inayat, S. Khan, B. Anthony, and V. Chang. 2017. "From Intrusion Detection to an Intrusion Response System: Fundamentals, Requirements, and Future Directions." *Algorithms* 10 (2): 39. https://doi.org/10.3390/a10020039.

Banjo, O. 2024. “Enhancing Cybersecurity through Comprehensive User Training Programs: A Study on Mitigating Social Engineering Threats.” *NORMA@NCI Library*. https://norma.ncirl.ie/7734/1/olumideoladapobanjo.pdf.

Barnea, A. 2019. “Big Data and Counterintelligence in Western Countries.” *International Journal of Intelligence and CounterIntelligence* 32 (3): 433–447. https://doi.org/10.1080/08850607.2019.1605804.

Beckers, K., and S. Pape. 2016. “A Serious Game for Eliciting Social Engineering Security Requirements.” https://mediatum.ub.tum.de/doc/1328974/1328974.pdf.

Beckers, K., V. Fries, E. Groen, and S. Pape. 2017. “Creativity Techniques for Social Engineering Threat Elicitation: A Controlled Experiment.” https://ceur-ws.org/Vol-1796/creare-paper-1.pdf.

Beneda, J., and S. L. Jaros. 2020. “The PAR Capabilities and the Convergence of Workplace Violence Prevention, Counter-Insider Threat, and Personnel Vetting Policies in DoD.” https://apps.dtic.mil/sti/html/tr/AD1094489/index.html.

Bhavsar, V., A. Kadlak, and S. Sharma. 2018. “Study on Phishing Attacks.” *International Journal of Computer Applications* 182 (33): 27–29. https://www.ijcaonline.org/archives/volume182/number33/30244-2018918286/.

Breda, F., H. Barbosa, and T. Morais. 2017. “Social Engineering and Cyber Security.” *INTED2017 Proceedings* 1: 4204–4211. https://www.scirp.org/reference/referencespapers?referenceid=3347298.

Bullée, J. W. H., L. Montoya, W. Pieters, M. Junger, and P. H. Hartel. 2015. “The Persuasion and Security Awareness Experiment: Reducing the Success of Social Engineering Attacks.” *Journal of Experimental Criminology* 11 (1): 97–115. https://doi.org/10.1007/s11292-014-9222-7.

___. 2017. “On the Anatomy of Social Engineering Attacks—A Literature-Based Dissection of Successful Attacks.” *Journal of Investigative Psychology and Offender Profiling* 15 (1): 20–45. https://doi.org/10.1002/jip.1482.

Cheh, C., U. Thakore, B. Chen, W. Temple, and W. Sanders. 2019. “Leveraging Physical Access Logs to Identify Tailgating: Limitations and Solutions.” https://www.perform.illinois.edu/Papers/USAN_papers/19CHE01.pdf.

Chen, Y., K. Ramamurthy, and K. W. Wen. 2019. “Impacts of Comprehensive Information Security Programs on Information Security Culture.” *Journal of Computer Information Systems* 55 (3): 11–19. https://doi.org/10.1080/08874417.2015.11645767.

Cho, I., and K. Lee. 2016. “Advanced Risk Measurement Approach to Insider Threats in Cyberspace.” *Intelligent Automation & Soft Computing* 22 (3): 405–413. https://doi.org/10.1080/10798587.2015.1121617.

Cooke, N. J. 1994. “Varieties of Knowledge Elicitation Techniques.” *International Journal of Human-Computer Studies* 41 (6): 801–849. https://doi.org/10.1006/ijhc.1994.1083.

Eminağaoğlu, M., E. Uçar, and Ş. Eren. 2009. “The Positive Outcomes of Information Security Awareness Training in Companies – A Case Study.” *Information Security Technical Report* 14 (4): 223–229. https://doi.org/10.1016/j.istr.2010.05.002.

Erbschloe, M. 2020. *Social Engineering: Hacking Systems, Nations, and Societies*. CRC Press, Taylor & Francis Group.

Foryst, C. A. 2010. "Rethinking National Security Strategy Priorities." *International Journal of Intelligence and CounterIntelligence* 23 (3): 399–425. https://doi.org/10.1080/08850600903566165.

Georgiadou, A., S. Mouzakitis, and D. Askounis. 2021. "Detecting Insider Threat via a Cyber-Security Culture Framework." *Journal of Computer Information Systems* 62 (4): 1–11. https://doi.org/10.1080/08874417.2021.1903367.

Gray, J. 2021. *Practical Social Engineering: A Primer for the Ethical Hacker*. San Francisco: No Starch Press.

Hadnagy, C. 2018. *Social Engineering: The Science of Human Hacking*. Indianapolis, IN: Wiley.

Hatfield, J. M. 2018. "Social Engineering in Cybersecurity: The Evolution of a Concept." *Computers & Security* 73: 102–113. https://doi.org/10.1016/j.cose.2017.10.008.

Jakobsson, M. 2018. *Understanding Social Engineering Based Scams*. Cham: Springer.

Johnson, L. K. 2010. *Handbook of Intelligence Studies*. London: Routledge.

Kanellopoulos, A. N. 2022. "The Importance of Counterintelligence Culture in State Security." *Global Security and Intelligence Note* 1 (5). https://www.buckingham.ac.uk/research/bucsis/hub/gsin/library/.

___. 2023. "The Dimensions of Counterintelligence and Their Role in National Security." *Journal of European and American Intelligence Studies* 6 (2).

___. 2024a. "Counterintelligence, Artificial Intelligence and National Security: Synergy and Challenges." *Journal of Politics and Ethics in New Technologies and AI* 3 (1): e35617–e35617. https://doi.org/10.12681/jpentai.35617.

_
__. 2024b. "Insider Threat Mitigation through Human Intelligence and Counterintelligence: A Case Study in the Shipping Industry." *Defense and Security Studies* 5: 10–19. https://doi.org/10.37868/dss.v5.id261.

Kuloğlu, G., Z. Gül, and Ş. Ş. Erçetin. 2014. "Counter-Intelligence as a Chaotic Phenomenon and Its Importance in National Security." In *Understanding Complex Systems*, 171–88. https://doi.org/10.1007/978-94-017-8691-1_11.

Matyokurehwa, K., N. Rudhumbu, C. Gombiro, and C. Chipfumbu-Kangara. 2022. "Enhanced Social Engineering Framework Mitigating against Social Engineering Attacks in Higher Education." *Security and Privacy*. https://doi.org/10.1002/spy2.237.

Moyers, R. 2025. "Deconstructing and Reconstructing Strategic Counterintelligence Toward a New Model." *Studies in Intelligence* 69 (2). https://www.cia.gov/resources/csi/static/Article-Moyers-Strategic-Counterintelligence-June-2025-1.pdf.

Poehlmann, N., K. M. Caramancion, I. Tatar, Y. Li, M. Barati, and T. Merz. 2021. "The Organizational Cybersecurity Success Factors: An Exhaustive Literature Review." In *Advances in Security, Networks, and Internet of Things*, 377–95. https://doi.org/10.1007/978-3-030-71017-0_27.

Prunckun, Harry. 2019. *Counterintelligence Theory and Practice*. Rowman & Littlefield.

Reynolds, Vincent. 2016. *Social Engineering: The Art of Psychological Warfare, Human Hacking, Persuasion & Deception*. Createspace.

Salama, R., and Fadi Al-Turjman. 2023. "Cyber-Security Countermeasures and Vulnerabilities to Prevent Social-Engineering Attacks." In *CRC Press EBooks*, 133–44. https://doi.org/10.1201/9781003322887-7.

Schaab, Philipp, Karsten Beckers, and Sebastian Pape. 2017. "Social Engineering Defence Mechanisms and Counteracting Training Strategies." *Information and Computer Security* 25 (2): 206–22. https://doi.org/10.1108/ics-04-2017-0022.

Sharma, Prakash, Bibhudutta Dash, and Mohammed F. Ansari. 2022. "Anti-Phishing Techniques – A Review of Cyber Defense Mechanisms." *Social Science Research Network*. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4335354.

Shulsky, Abram N., and Gary J. Schmitt. 2009. *Silent Warfare: Understanding the World of Intelligence*. Potomac Books, Inc.

Siddiqi, Muhammad A., Won Pak, and Muhammad A. Siddiqi. 2022. "A Study on the Psychology of Social Engineering-Based Cyberattacks and Existing Countermeasures." *Applied Sciences* 12 (12): 6042. https://doi.org/10.3390/app12126042.

Sims, Jennifer E., and Burton L. Gerber. 2009. *Vaults, Mirrors, and Masks: Rediscovering U.S. Counterintelligence*. Center for Peace and Security Studies – Georgetown University Press.

Sithole, Themba, and Johann Du Toit. 2022. "A Cyber Counterintelligence Competence Framework." *European Conference on Cyber Warfare and Security* 21 (1): 368–77. https://doi.org/10.34190/eccws.21.1.255.

Sobur, Abdus, A. Hossain, Kazi Nazrul Islam, and Md Humayun Kabir. 2024. "A Contradistinction Study of Physical vs. Cyberspace Social Engineering Attacks and Defense." *SSRN Electronic Journal*. https://doi.org/10.2139/ssrn.4878111.

Stavrou, Vasilis, Michalis Kandias, Georgios Karoulas, and Dimitris Gritzalis. 2014. "Business Process Modeling for Insider Threat Monitoring and Handling." In *Trust, Privacy, and Security in Digital Business*, 119–31. https://doi.org/10.1007/978-3-319-09770-1_11.

Stouder, Michael D., and Sean Gallagher. 2013. "Crafting Operational Counterintelligence Strategy: A Guide for Managers." *International Journal of Intelligence and CounterIntelligence* 26 (3): 583–96. https://doi.org/10.1080/08850607.2013.780560.

Subhani, A., I. A. Khan, and A. Zubair. 2021. "Review of Insider and Insider Threat Detection in the Organizations." *Journal of Advanced Research in Social Sciences and Humanities* 6 (4). https://doi.org/10.26500/jarssh-06-2021-0402.

Syafitri, W., Z. Shukur, U. A. Mokhtar, R. Sulaiman, and M. A. Ibrahim. 2022. "Social Engineering Attacks Prevention: A Systematic Literature Review." *IEEE Access* 10 (1): 39325–39343. https://doi.org/10.1109/ACCESS.2022.3162594.

Tiwari, S., and S. S. Rathore. 2017. "A Methodology for the Selection of Requirement Elicitation Techniques." arXiv. https://arxiv.org/abs/1709.08481.

Volini, A. 2021. "A Deep Dive into Technical Encryption Concepts to Better Understand Cybersecurity & Data Privacy Legal & Policy Issues." *Digital Commons @ University of Georgia School of Law*. https://digitalcommons.law.uga.edu/jipl/vol28/iss2/2/.

Wang, D., and P. Wang. 2016. "Two Birds with One Stone: Two-Factor Authentication with Security Beyond Conventional Bound." *IEEE Transactions on Dependable and Secure Computing* 15 (4). https://doi.org/10.1109/tdsc.2016.2605087.

Wang, P., and P. Lutchkus. 2023. "Psychological Tactics of Phishing Emails." *Issues in Information Systems* 24 (2). https://doi.org/10.48009/2_iis_2023_107.