SHODH SAMAGAM

ISSN : 2581-6918 (Online), 2582-1792 (PRINT)

Honey-Trap Espionage in India: A Psychological Perspective through Content Analysis of National-Level Cases

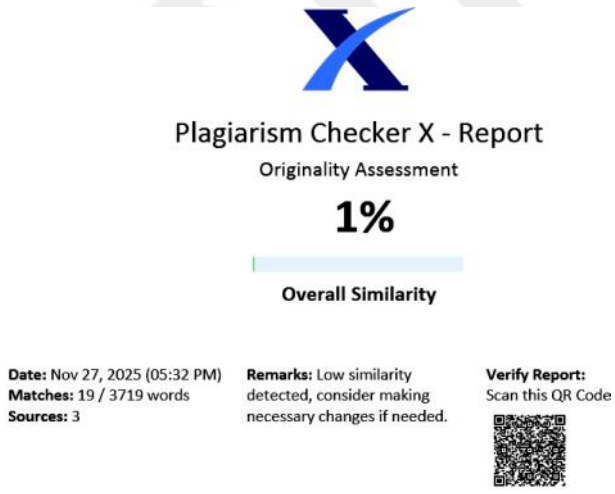
Anmol Shekhar Srivastava, Department of Clinical Psychology
Chhatrapati Shahu Ji Maharaj University, Kanpur, Uttar Pradesh, INDIA
Akhilesh Dwivedi
Kanpur, Uttar Pradesh, INDIA

ORIGINAL ARTICLE

Authors
Anmol Shekhar Srivastava
Akhilesh Dwivedi
E-mail : anmol@csjmu.ac.in

shodhsamagam1@gmail.com

Received on : 26/09/2025
Revised on : 26/11/2025
Accepted on : 05/12/2025
Overall Similarity : 01% on 27/11/2025



ABSTRACT

Honey-trap espionage, involving emotional, romantic, or sexual manipulation for extracting classified information, has re-emerged as a critical national security threat in India in the digital era. While widely reported in strategic and media discourse, its psychological foundations remain under-examined in academic research. This study addresses that gap by conducting a qualitative content analysis of five major, publicly documented Indian honey-trap espionage cases between 2010 and 2024, including incidents involving defence scientists, military personnel, and diplomatic staff. Drawing on verified sources such as court documents, official statements, and credible national media reports, the analysis identifies recurring psychological vulnerabilities, including loneliness, ego involvement, need for validation, online disinhibition, and emotional dependency. These vulnerabilities are systematically exploited using persuasion and grooming strategies like flattery, gradual trust-building, reciprocity, and subsequent coercion or blackmail. The findings reveal that honey-trapping operates not merely through operational lapses, but through a psychological interplay between human vulnerabilities and digital affordances. Based on cross-case thematic coding, the study proposes a vulnerability-based typology of honey-trap manipulation strategies in the Indian context, integrating concepts from persuasion theory, cognitive dissonance, moral disengagement, and online disinhibition. By bridging psychological theory with national security perspectives, this research contributes to defence psychology and

counterintelligence studies and highlights the need for psychologically informed training, resilience-building, and early behavioural risk detection among sensitive personnel in national security institutions.

KEY WORDS

Honey-trap, Espionage, Persuasion, Insider Vulnerability, Defence Studies, Content Analysis..

INTRODUCTION

Honey-trap espionage refers to the use of emotional, romantic, or sexual manipulation,real or simulated,to induce individuals into revealing classified or sensitive information, or to make them vulnerable to blackmail and coercion (Bukhari et al., 2025; Wilder, 2017). In the contemporary digital environment, this tradecraft has evolved beyond physical proximity into online spaces such as social media, encrypted messaging platforms, and professional networks, where anonymous or staged identities can initiate prolonged psychological grooming with minimal risk of detection.

In India, a series of recent high-profile espionage cases involving defence scientists, military officers, and diplomatic personnel have drawn renewed attention to honey-trapping as a national security concern (Indian Express, 2023; Hindustan Times, 2024). These cases reveal a consistent pattern: online contact initiated by foreign operatives, followed by emotional engagement, gradual trust-building, and ultimately, information extraction or coercion under the Official Secrets Act. While strategic and intelligence analyses often focus on operational failures and security breaches, such incidents highlight a deeper psychological dimension,how human vulnerabilities are systematically exploited within digitally mediated relationships.

Although global research has examined honey-trapping, romance fraud, social engineering, and insider threats, India-specific academic work that integrates psychological theory with documented national-level honey-trap cases remains limited (Wilder, 2017; Coluccia et al., 2020; Lazarus et al., 2023). Existing discussions are often journalistic or purely strategic, leaving a gap in understanding how psychological vulnerabilities, persuasion techniques, and organisational contexts interact in Indian cases of honey-trap espionage.

Addressing this gap, the present study conducts a qualitative content analysis of five major Indian honey-trap espionage cases between 2010 and 2024 involving personnel from defence, diplomatic, and paramilitary institutions. The study seeks to (a) identify recurrent psychological vulnerabilities such as loneliness, ego involvement, need for validation, and online disinhibition; (b) examine common persuasion and manipulation tactics such as grooming, flattery, reciprocity, and coercion; and (c) analyse how these psychological factors interact with organisational roles, access levels, and digital platforms to facilitate espionage.

By integrating insights from persuasion theory, insider-threat literature, cognitive dissonance research, and cyber-psychology, this study develops an India-specific, psychologically grounded typology of honey-trap mechanisms relevant to contemporary national security challenges. The findings aim to contribute to both defence psychology and counterintelligence practice by providing empirically informed insights for psychological screening, awareness training, and preventive intervention within sensitive government and defence institutions.

Literature Review

Honey-trapping, defined as the use of emotional, romantic, or sexual manipulation to extract sensitive information or coerce cooperation, remains a persistent human-factor vulnerability in intelligence operations. Espionage research consistently shows that such betrayal arises from the interaction of psychological vulnerability, situational stressors, and access opportunity (Wilder, 2017). Contemporary honey-traps exploit fundamental human needs for attachment, validation, status, and security, while leveraging digital platforms that enable identity fabrication, continuous contact, and narrative control. This fusion of psychological susceptibility and digital affordances has made honey-trapping especially effective in modern intelligence environments.

Psychological research demonstrates that individuals experiencing loneliness, emotional isolation, or unmet affiliation needs are more susceptible to simulated intimacy. Online romance fraud studies show that perpetrators invest weeks or months in establishing trust and emotional bonds before introducing exploitative demands (Coluccia et al., 2020; Whitty, 2018). Such grooming activates attachment systems, lowering cognitive resistance and increasing dependency. In high-stress organisational contexts such as defence and intelligence, where long postings and emotional isolation are common, this vulnerability is intensified. Additionally, ego involvement and the need for professional validation, especially among high-status technical personnel, further increase susceptibility to manipulation through flattery and admiration (Sedikides & Gregg, 2008).

Honey-trap operations function through established persuasion and social engineering principles such as liking, reciprocity, commitment, and scarcity (Cialdini, 2001; Washo, 2021). Research on cyber-social engineering and romance fraud illustrates a structured progression: initial contact, rapport building, trust development, emotional investment, and eventual extraction (Coluccia et al., 2020; Whitty, 2018; Khadka, 2024). Digital disinhibition further strengthens this process by reducing self-monitoring and increasing emotional risk-taking in online environments (Suler, 2004). Victims often ignore warning signs due to emotional investment and cognitive bias (Lazarus et al., 2023; Coluccia et al., 2020).

Once exploitation begins, moral disengagement and rationalisation mechanisms facilitate continued compliance. Targets minimise their actions ("I only shared minimal information"), diffuse responsibility, and gradually normalise boundary violations (Wilder, 2017). Bandura's (1999) moral disengagement framework explains how individuals cognitively reduce internal moral conflict by reframing harmful actions. Increasing emotional and behavioural commitment further leads to cognitive dissonance, delaying disclosure and deepening organisational risk (Lazarus et al., 2023; Whitty, 2018).

The insider-threat literature complements this understanding by identifying behavioural and psychological precursors to betrayal, including financial stress, social withdrawal, personality traits like impulsivity and sensation-seeking, and irregular access patterns (Greitzer & Frincke, 2010; SoK: The Psychology of Insider Threats, 2025). Crucially, access remains a decisive factor: even minor disclosures can become catastrophic when the target holds high-level clearance or strategic roles.

Strategic studies highlight that in the era of digital warfare and hybrid threats, honey-trapping has evolved into a scalable, state-level intelligence tool. Digital environments allow operatives to target multiple individuals simultaneously, maintain plausible deniability through fake personas, and use OSINT to psychologically tailor their approach (Bukhari, 2025). Consequently, scholars emphasise that counter-honey-trap strategies must integrate psychological training, digital risk awareness, and behavioural monitoring rather than relying solely on technical security protocols.

In the Indian context, multiple high-profile cases involving DRDO scientists, BrahMos engineers, diplomats, and defence personnel follow a consistent trajectory: online contact, emotional grooming, gradual trust escalation, and eventual disclosure under emotional or coercive pressure (Indian Express, 2023; LiveMint, 2023; Hindustan Times, 2024). While global literature on social engineering and insider threats is extensive, systematic, India-focused psychological analyses of honey-trap espionage cases remain limited. Most existing Indian accounts are journalistic or strategic, lacking structured psychological coding and theoretical integration. However, available case narratives provide rich material for content analysis and typology building.

Overall, the literature converges across three domains: (a) psychological research on emotional manipulation, persuasion, and romance fraud; (b) insider-threat frameworks identifying behavioural risk markers; and (c) strategic analyses of honey-trap operations in digital warfare contexts. What remains missing is an India-centric psychological synthesis integrating these strands through empirical case analysis. The present study addresses this gap by applying an integrated psychological–tradecraft framework to Indian honey-trap espionage cases, aiming to develop a culturally grounded typology and evidence-based counterintelligence intervention model (The Indian Express, 2025).

Methodology

Research Design

This study employs a qualitative content analysis approach to examine the psychological mechanisms underlying honey-trap espionage cases in India. Following Mayring's (2014) structured qualitative framework, both manifest (observable) behaviours and latent (psychological) meanings were analysed across selected case materials.

Data Sources and Case Selection

Data were drawn from publicly available, verified sources, including court documents, government statements, and credible national media coverage. These were supplemented by peer-reviewed literature and official open-source intelligence materials.

Five national-level Indian honey-trap espionage cases (2010–2024) were selected using purposive sampling based on three criteria:

1. Involvement of defence, security, or diplomatic personnel.
2. Documented link to espionage or national security compromise.
3. Availability of sufficient narrative detail to analyse psychological processes.

The sample includes cases involving a DRDO scientist, embassy official, Indian Air Force officer, BSF jawan, and a senior diplomat, ensuring variation across organisational levels and roles.

Data Coding and Analytical Framework

A theory-driven codebook was developed using constructs from persuasion theory, insider-threat literature, and cyber-psychology. Data were coded and analysed using NVivo 14.

To maintain analytical focus, the codebook was condensed to the following six core psychological categories:

Code	Description	Theoretical Basis
Emotional Grooming	Building emotional trust and attachment prior to exploitation	Attachment theory; Grooming models
Ego Reinforcement	Manipulating pride, status, or self-image	Self-enhancement theory; Cialdini's liking principle
Loneliness & Validation Need	Exploiting social isolation and emotional dependency	Maslow's belongingness needs
Reciprocity & Gradual Disclosure	Escalating compliance through small exchanges	Social exchange theory
Fear Conditioning / Blackmail	Use of threats and coercion to enforce compliance	Operant conditioning
Online Disinhibition	Reduced self-regulation due to digital anonymity	Suler's (2004) model

Data Analysis Procedure

Thematic content analysis was conducted in three stages:

1. Open coding of psychological and behavioural indicators.
2. Grouping of codes into broader vulnerability and manipulation themes.
3. Cross-case comparison to identify recurring patterns and typological structures.

Ethical Considerations

All data were derived from public, open-access sources, and no confidential or classified materials were used. No direct human participants were involved. Personal identifiers were handled with sensitivity,

and references to individuals were restricted to publicly documented material. The study followed standard research ethics guidelines of the APA (2023) and national research integrity norms of India.

Reliability and Validity

Reliability was supported through multi-source triangulation and dual coding. Validity was ensured by grounding interpretations in established psychological frameworks and cross-referencing findings with existing research on espionage psychology and insider threats.

Results and Discussion

1. Emotional Grooming and Trust Manipulation

Across all five cases, emotional grooming emerged as the primary entry mechanism into espionage. Handlers initiated prolonged interpersonal engagement using flattery, empathy, and romantic cues to create a perception of authenticity and intimacy. In the Kurulkar (2023) and Siwal (2024) cases, perpetrators maintained daily contact over extended periods, gradually shifting from casual communication to emotionally charged conversations. This process weakened professional boundaries and reduced critical judgment, as victims began to view interactions as personal rather than suspicious.

Rather than using immediate coercion, handlers relied on sustained emotional investment, generating psychological dependency before introducing sensitive requests. The BSF Jawan (2016) and Indian Air Force officer (2018) cases illustrate how digital communication platforms created a false sense of closeness and trust, despite no physical interaction. Emotional involvement thus acted as the gateway vulnerability, enabling later stages of compliance and exploitation. This confirms that honey-trapping in the Indian context operates primarily as a psychological grooming process, not a sudden act of seduction or coercion.

2. Ego Reinforcement, Loneliness, and Validation Needs

A second dominant vulnerability across cases was the combination of ego involvement and emotional isolation. Senior personnel such as DRDO scientists and diplomatic staff displayed sensitivity to flattery framed around professional competence, patriotism, and strategic importance. Handlers exploited this by positioning themselves as admirers, intellectual equals, or emotionally supportive figures. In the Kurulkar and Air Force cases, praise for intelligence and contribution to national defence reinforced a sense of personal significance, lowering resistance to engagement.

At the same time, social isolation, due to long postings, secrecy of occupation, or personal life stress, created a psychological vacuum. The BSF Jawan and Siwal cases reflect how loneliness and lack of emotional support outside work increased susceptibility to online intimacy. Once validation needs were activated, relationships were experienced as meaningful rather than deceptive. Thus, honey-trapping was less about sexual attraction and more about emotional affirmation and perceived recognition, particularly in individuals whose identity was strongly linked to professional roles.

3. Gradual Disclosure and Coercive Escalation

A clear behavioural pattern across cases was incremental disclosure, where handlers first requested harmless or non-sensitive information before escalating to classified material. In the Siwal (2024) case, early communication involved general embassy-related content, gradually progressing to sensitive operational details. Once minor disclosures occurred, victims experienced psychological consistency pressure, making refusal of later requests increasingly difficult.

In several cases, this stage transitioned into coercive control, especially when compromising material had been obtained. The BSF Jawan case clearly illustrates this progression: once private images and emotional vulnerabilities were captured, blackmail and threats replaced affection. Victims complied not due to continued persuasion but due to fear of social, personal, and professional exposure. This shift from voluntary grooming to coerced compliance marks a critical transition phase in honey-trap operations, reinforcing their classification as both psychological manipulation and behavioural entrapment.

4. Rationalisation and Psychological Entrapment

The final stage across cases involved cognitive rationalisation and moral disengagement. In the Madhuri Gupta (2010) case, emotional involvement merged with ideological reinterpretation, allowing betrayal to be reframed as empathy or peace-building. Other cases reflected similar rationalisations, with individuals minimising the impact of their actions ("It was not significant information") or diffusing responsibility ("I was emotionally pressured").

As disclosures increased, victims became psychologically entrapped, not just by handlers but by their own fear, shame, and self-justification. This explains why reporting was delayed or completely absent in most cases until external agencies intervened. Rather than ideological disloyalty, the dominant psychological process was progressive moral disengagement under emotional and situational pressure. The cases demonstrate that once individuals cross initial ethical boundaries, psychological investment and fear create a self-reinforcing cycle of continued compliance and silence.

Cross-Case Integrative Pattern

Across all five cases, the following psychological trajectory consistently emerged:

This sequence illustrates that honey-trap espionage in India is less about sudden betrayal and more about gradual psychological erosion under emotional manipulation. The findings strongly support the argument that human vulnerability, not technical or ideological failure alone, remains the weakest link in national security systems.

Policy and Broader Implications

1. Psychologically Informed Training

Traditional counterintelligence training in India is largely procedure- and protocol-driven, with limited emphasis on the emotional and psychological dimensions of manipulation. The findings of this study suggest that personnel in sensitive positions require psychology-based awareness training focused specifically on grooming dynamics, emotional exploitation, and persuasion tactics used in honey-traps. Training modules should incorporate realistic case simulations, behavioural role-plays, and digital grooming scenarios, enabling staff to recognise early-stage manipulation patterns rather than only overt security breaches.

2. Digital Risk Awareness and Behavioural Protocols

Given that most contemporary honey-trap operations originate online, digital platforms constitute a primary vulnerability zone. Defence institutions must implement structured digital conduct guidelines and education programmes that address risks associated with social media use, online intimacy, and private messaging platforms. Awareness initiatives should go beyond technical cyber hygiene and focus on emotional self-regulation, online disinhibition, and social engineering techniques. Special attention is required for personnel stationed in socially isolated or high-stress environments, where vulnerability is elevated.

3. Psychological Screening and Insider Risk Tools

Standard security vetting procedures often prioritise background checks and financial risk indicators, while undervaluing psychological risk markers such as loneliness, ego vulnerability, emotional instability, and impulsivity. The study recommends the integration of periodic psychological assessment tools, focusing on emotional resilience, interpersonal boundaries, and susceptibility to manipulation, within high-security clearance procedures. However, such screening must be framed as preventive and supportive, not punitive, to avoid stigma and concealment.

4. Institutional Support and Reporting Culture

A critical finding across cases was delayed disclosure due to shame, fear of punitive action, and reputational damage. Therefore, institutions must foster non-punitive, confidential reporting mechanisms for suspicious contacts and psychological compromise. This should be accompanied by counselling support and post-report protection, ensuring that early reporting is incentivised rather than discouraged. Without trust in institutional support systems, even highly trained professionals remain unlikely to disclose vulnerability until irreversible damage has occurred.

Limitations and Future Research Directions

This study relies solely on publicly available court records, media reports, and open-source materials, which may lack classified operational details necessary for a fuller ïñèõîëîãical reconstruction. Many honey-trap cases remain undisclosed due to security concerns and stigma, meaning the analysed cases likely represent only a small visible proportion, limiting generalisability. Moreover, the findings are rooted in the Indian defence and cultural context and should be cautiously applied to other settings. Future research should use mixed methods, include expert and practitioner inputs, and adopt cross-national comparisons to strengthen both depth and applicability.

CONCLUSION

The present content analysis demonstrates that honey-trap espionage in India functions less through physical seduction and more through psychological orchestration. Emotional manipulation, ego reinforcement, loneliness alleviation, and moral rationalisation together create a fertile psychological environment for betrayal. These cases reveal a distinct transition from romance to coercion, where affection becomes the entry point and fear sustains compliance.

Ultimately, the findings affirm that espionage is not merely a geopolitical act but a psychological one. It operates through the subtle erosion of judgment and the systematic capture of trust. In modern digital ecosystems, where intimacy and deception coexist seamlessly, the mind emerges as the true battlefield, and trust, the most potent weapon. Thus, strengthening psychological literacy, resilience, and emotional regulation among defence personnel is not just a mental health initiative but a strategic necessity for national security.

REFERENCES

1. Bandura, A. (1999) Moral disengagement in the perpetration of inhumanities, *Personality and Social Psychology Review,* 3(3), 193–209. https://doi.org/10.1207/s15327957pspr0303_3
2. Braun, V. & Clarke, V. (2006) Using thematic analysis in psychology, *Qualitative Research in Psychology,* 3(2), 77–101. https://doi.org/10.1191/1478088706qp063oa
3. Baumeister, R. F. & Leary, M. R. (1995) The need to belong: Desire for interpersonal attachments as a fundamental human motivation, *Psychological Bulletin*, 117(3), 497–529. https://doi.org/10.1037/0033-2909.117.3.497
4. Bowlby, J. (1988) *A secure base: Parent-child attachment and healthy human development,* Basic Books, New York, NY.
5. Bukhari, S. R. H.; Irshad, A. U. R. B. & Khan, E. (2025) Honey trap espionage in the age of digital warfare: Strategic lessons from India's DRDO scandal and implications for Pakistan's national security, *Qlantic Journal of Social Sciences and Humanities*, 6(3), 1–13. https://doi.org/10.55737/qjssh.vi-iii.25379
6. Central Intelligence Agency. (2025) CIA Reading Room, Retrieved from https://www.cia.gov/readingroom/, Accessed on 24/09/2025.

7. Charney, D. L. (2014) True psychology of the insider spy. National Insider Threat Special Interest Group. Retrieved from https://www.nationalinsiderthreatsig.org/itrmresources/True%20Psychology%20Of%20Insider%20Spy-By%20David%20Charney.pdf, Accessed on 24/09/2025.
8. Cialdini, R. B. (2001) *Influence: Science and practice*, (4th ed.) Allyn & Bacon, Boston, MA.
9. Cialdini, R. B. (2016) Pre-suasion: A revolutionary way to influence and persuade, Simon & Schuster, New York, NY.
10. Coluccia, A.; Pozza, A.; Ferretti, F.; Carabellese, F.; Masti, A. & Gualtieri, G. (2020) Online romance scams: Relational dynamics and psychological characteristics of the victims and scammers - A scoping review, *Clinical Practice and Epidemiology in Mental Health*, 16, 24–35. https://doi.org/10.2174/1745017902016010024
11. DRDO scientist honey trap case: ATS chargesheet reveals sharing of Indian missile, drone details with Pakistani operative. (2023, April 18) Hindustan Times. Retrieved from https://www.hindustantimes.com/cities/mumbai-news/pune-scientist-arrested-for-espionage-shared-sensitive-missile-and-drone-details-with-pakistani-operative-101688757246133.html, Accessed on 24/09/2025.
12. Festinger, L. (1957) *A theory of cognitive dissonance*, Stanford University Press, Stanford, CA.
13. Freedman, J. L. & Fraser, S. C. (1966) Compliance without pressure: The foot-in-the-door technique, *Journal of Personality and Social Psychology*, 4(2), 195–202. https://doi.org/10.1037/h0023552
14. Greitzer, F. L. & Frincke, D. A. (2010) Combining traditional cyber security audit data with psychosocial data: Towards predictive modelling for insider threat mitigation. In Insider Threats in Cyber Security, p. 85–113, Springe, Boston, MA, https://doi.org/10.1007/978-1-4419-7133-3_5
15. Hillsberg, R. (2024) Agent handling 101: The psychology of running spies. SPYSCAPE Retrieved from https://spyscape.com/article/agent-handling-101-the-psychology-of-running-spies, Accessed on 24/09/2025.
16. Hindustan Times (2024, June 4) Former BrahMos engineer sentenced to life for spying, https://www.hindustantimes.com/india-news/former-brahmos-engineer-sentenced-to-life-for-spying-101717437821776.html, Accessed on 24/09/2025.
17. Honeytraps and high treason: The faces behind India's spy scandals. (2025, May 20) India Today, Retrieved from https://www.indiatoday.in/india/story/honeytraps-and-high-treason-the-faces-behind-indias-spy-scandals-2727654-2025-05-20, Accessed on 23/09/2025.
18. Horgan, J. (2012) *The psychology of terrorism*, Routledge, New York, NY.
19. Indian Express (2023, August 2) DRDO espionage case: Scientist files bail plea, claims info 'shared with Pak woman' was in public domain, The Indian Express, https://indianexpress.com/article/cities/pune/drdo-espionage-case-scientist-bail-plea-info-pakistan-woman-public-domain-8873249/, Accessed on 20/09/2025.
20. Indian Express (2023, June 30) Espionage case: ATS files chargesheet against Kurulkar; DRDO scientist refuses polygraph test, https://indianexpress.com/article/cities/pune/pune-espionage-case-ats-chargesheet-drdo-scientist-refuses-polygraph-8694480/, Accessed on 18/09/2025.

21. Khadka, K. (2024) A survey on the principles of persuasion as a social engineering tool, arXiv. https://arxiv.org/abs/2412.18488, Accessed on 24/09/2025.
22. Lazarus, S.; Whittaker, J. M.; McGuire, M. R. & Platt, L. (2023) What do we know about online romance fraud studies? A systematic review of the empirical literature (2000–2021) *Journal of Economic Criminology, Volume, Issue & Page Number ???,* 100013. https://doi.org/10.1016/j.jeconc.2023.100013
23. Livemint (2023, July 8) Honey-trapped DRDO scientist Kurulkar attracted to Pakistani agent, discussed Indian missile systems: Chargesheet, LiveMint, https://www.livemint.com/news/world/honeytrapped-drdo-scientist-kurulkar-attracted-to-pakistani-agent-discussed-indian-missile-systems-chargesheet-11688790604549.html, Accessed on 19/09/2025.
24. Maslow, A. H. (1943) A theory of human motivation, *Psychological Review,* 50(4), 370–396. https://doi.org/10.1037/h0054346
25. Mayring, P. (2014) Qualitative content analysis: Theoretical foundation, basic procedures and software solution, Beltz Verlag, Klagenfurt.
26. McCormick, R. (2020) Emotional manipulation and digital intimacy: The modern honey trap, *Journal of Cyber-Psychology,* 14(2), 89–104. https://doi.org/10.1037/cyb0000203
27. Miron, M. (n.d.) The psychology of a modern spy. CIA, Retrieved from https://www.cia.gov/readingroom/docs/CIA-RDP90-00965R000706200002-8.pdf, Accessed on 17/09/2025.
28. Rid, T. & Buchanan, B. (2015) Attributing cyber attacks, *Journal of Strategic Studies*, 38(1–2), 4–37. https://doi.org/10.1080/01402390.2014.977382
29. Schafer, J. R. & Navarro, J. (2020) The truth detector: An ex-FBI agent's guide for getting people to reveal the truth. Scribner, New York, NY.
30. Sedikides, C. & Gregg, A. P. (2008) Self-enhancement: Food for thought, *Perspectives on Psychological Science*, 3(2), 102–116. https://doi.org/10.1111/j.1745-6916.2008.00068.x
31. Skinner, B. F. (1953) Science and human behavior. Macmillan.
32. Stark, E. (2007) Coercive control: How men entrap women in personal life, Oxford University Press, New York, NY.
33. Suler, J. (2004) The online disinhibition effect, *Cyber Psychology & Behavior,* 7(3), 321–326. https://doi.org/10.1089/1094931041291295
34. Tavris, C. & Aronson, E. (2020) Mistakes were made (but not by me): Why we justify foolish beliefs, bad decisions, and hurtful acts, Mariner Books, New York, NY.
35. The Times of India (2024, June) Ex-BrahMos engineer gets 14 years' jail for leaking data to Pakistan, https://timesofindia.indiatimes.com/india/ex-brahmos-engineer-gets-14-years-jail-for-leaking-data-to-pakistan/articleshow/110677702.cms, Accessed on 15/09/2025.
36. Whitty, M. T. (2018) Do you love me? Psychological characteristics of romance scam victims, *Journal of Criminal Psychology,* 8(2), 139–151. https://doi.org/10.1108/JCP-09-2016-0032
37. Wilder, U. M. (2017) The psychology of espionage. Studies in Intelligence, 61(2) Central Intelligence Agency. https://www.cia.gov/resources/csi/static/psychology-of-espionage.pdf, Accessed on 15/09/2025.

****