KrimOJ Kriminologie – Das Online-Journal
Criminology – The Online Journal

No. 2/2024

Pranav Prakash, Surbhi Girdhar and Antony Jose

Deciphering Honey Trapping Crime Cases in India

The presence of Honey-trapping in different forms dates back to the time of ancient kingdoms and empires and involves utilizing romantic or personal connections as a means of obtaining knowledge or power. Honey-trapping crimes have taken on new dimensions in the modern period, particularly in the cyber world, where profiles on social media sites like Facebook and Twitter are used to befriend and then seduce targets into disclosing important information. This behaviour has become a serious problem that jeopardises personal safety and national security. This study analyses the honey-trapping Crime Cases to interrogate the methods and implication strategies of honey-trapping, highlighting its transition from physical seduction to digital manipulation. It also scrutinizes the legal and ethical challenges posed by honey-trapping, emphasizing the lack of robust legal mechanisms to address these crimes. Furthermore, the paper discusses preventive measures to equip individuals and organisations against such threats.

Keywords: Crime Prevention, Criminal Law, Cyber Espionage, Cybersecurity, Digital Manipulation, Honey Trapping

Entschlüsselung von Honey-Trapping-Kriminalitätsfällen in Indien

Das Vorhandensein von Honigfallen in verschiedenen Formen stammt aus der Zeit der alten Königreiche und Imperien und beinhaltet die Verwendung von romantischen oder persönlichen Verbindungen als Mittel zur Erlangung von Wissen oder Macht. Besonders in der Cyberwelt, wo Profile auf Social-Media-Seiten wie Facebook und Twitter genutzt werden, um Freundschaften zu schließen und dann Zielpersonen dazu zu verleiten, wichtige Informationen preiszugeben, hat die Honigfang-Kriminalität in der Neuzeit neue Dimensionen angenommen. Dieses Verhalten ist zu einem ernsthaften Problem geworden, das die persönliche und die nationale Sicherheit gefährdet. Diese Studie analysiert die Honigfallen Kriminalitätsfälle, um die Methoden und Implikationsstrategien des Honey-trapping zu hinterfragen und den Übergang von physischer Verführung zur digitalen Manipulation aufzuzeigen. Es werden auch rechtliche und ethische Herausforderungen untersucht, die mit der Honigfalle verbunden sind. Zudem wird auf das Fehlen solider rechtlicher Mechanismen zur Bekämpfung dieser Verbrechen hingewiesen. Darüber hinaus werden Präventionsmaßnahmen diskutiert, um Einzelpersonen und Organisationen gegen solche Bedrohungen wappnen.

Schlagwörter: Cybersecurity; Cyberspionage; Digitale Manipulation; Honey Trapping; Kriminalprävention; Strafrecht

https://doi.org/10.18716/ojs/krimoj/2024.2.1

1. Introduction

Honey-trapping is an investigative practice that traditionally involves the use of romantic or sexual relationships for interpersonal, political, or monetary purposes to obtain sensitive information. In espionage, it includes making contact with a target possessing valuable information and enticing them into a false relationship to glean information or exert influence (Gupta, 2023). In the cyber world, honey-trapping crimes have gained new dimensions on social media platforms like Facebook and Twitter, where profiles (often bots or honey traps) are used to befriend and later lure targets into divulging crucial information. This practice has become a significant concern, compromising individual safety and national security (Innefu, 2023). The practice of using romantic or intimate relationships to gain information or influence has been prevalent in India for centuries as in other countries, with its roots traced back to ancient kingdoms and empires. The allure of romantic entanglement and the potential for personal gain have made honey-trapping a particularly effective tool for extracting sensitive information from unsuspecting individuals. One of the earliest documented instances of honey-trapping in India occurred during the Mughal era (1526-1857). The Mughal emperor Akbar, known for his strategic intelligence gathering, employed a network of spies, including women, to gather information about his rivals and potential threats to his empire. In the 18th century, the British East India Company, which gradually gained control over much of India, also employed honey-trapping techniques to gain insights into local politics and social dynamics. The company's agents often used relationships with Indian women to gain access to influential figures and gather intelligence about potential uprisings or resistance movements (Dalrymple, 2002).

Nowadays, honey-trapping has evolved into a sophisticated and often dangerous practice, employed by both domestic and foreign intelligence agencies. Indian intelligence agencies have been known to use honey-trapping techniques to gather information about potential threats to national security, such as terrorist groups or foreign espionage rings. However, these methods have also been used for more nefarious purposes, such as blackmailing individuals or influencing political outcomes. The use of honey-trapping in India has raised concerns about privacy, security, and the potential for exploitation. In recent years, there have been several high-profile cases of individuals being blackmailed or harmed after falling victim to honey-trapping schemes. The study of honey-trapping is crucial in understanding its impact on modern cybersecurity, exploitable human vulnerability and espionage. It highlights the evolving nature of honey-trapping from physical interactions to digital platforms, where deceptive profiles and AI are used for gathering. Especially the use of AI will become a great challenge in this respect in the coming years. This practice poses severe threats, especially when defence personnel are targeted, as they hold sensitive information crucial for national security. Recent cases, like the honey-trapping of Indian Army personnel by Pakistan-based operatives or Iranian soldiers by Hamas, underscore the global reach and grave consequences of this tactic (Deuskar, 2023; Sawant, 2019). Studying honey-trapping helps in devising counter-strategies to detect and prevent such espionage activities. It involves using sophisticated models and algorithms to identify potential honey trap profiles (Innefu, 2023), employing forensic network analysis like Complex Event Processing (Kumara et al., 2024).

Honey-trapping, an old tactic of using seduction to gain information or influence, has been amplified in the digital age (Nosál, 2023). With the prevalence of social media, dating apps,

and online communication, honey trappers have gained easier access to potential targets, exploiting their vulnerabilities (Kinsale, 2023). By creating fake online personas, honey trappers lure unsuspecting individuals, gradually building trust and rapport (Lindley, 2023). Once trust is established, they may request favours, such as sharing confidential information or providing access to restricted systems (Dalmia, 2019). Blackmailing is another tool employed in honey trapping, threatening to release compromising photos or videos obtained through deception (Innefu, 2023). Honey trapping can have severe consequences, causing financial losses, reputational damage, and emotional distress (Nosál, 2023), and in some cases, even leading to prosecution for crimes committed under deception (Kinsale, 2023). To protect yourself from honey trapping, exercise caution when connecting with people online (Lindley, 2023), avoid sharing personal information (Dalmia, 2019), be wary of overly friendly individuals or those offering unrealistic favours (Innefu, 2023).

Cases of honeytrap crimes, which are frequently connected to espionage attempts, have also been reported in China. To get information or sway decisions, agents may target people in important positions. These cases frequently involve complex strategies and might have important political ramifications. Honey trap methods often involve an individual persuading or seducing another individual, usually with the goal of obtaining private information, funds, or other favours. Such methods may be employed for a variety of reasons in China and other regions of the world, such as business espionage, political influence, or personal gain (Mandarin, 2024).

In Russian espionage operations, honey trap operations are not uncommon; operatives use seduction to compromise targets for political benefit or to get sensitive information. There have been reports that criminal organisations and both foreign and local intelligence services use honey trap operations in Russia. To get important information or sway their actions, these operations may target people in positions of authority or influence, such as government officials, business executives, or politicians (OpIndia, 2024).

Even while they might not happen as frequently in the United States as they do in other nations, honey trapping crimes still occur. There have been reported instances of people being singled out for extortion or blackmail via romantic enticement, sometimes through social media or online dating services. Depending on the type of fraud and the harm inflicted, identical situations may be referred to as fraud, blackmail, extortion, or other applicable criminal offences in the United States. Such matters are normally handled by law enforcement organisations and court systems by the particular laws and rules that apply to respective areas of authority (Firstpost, 2022). Honey trapping crimes have also occurred in the United Kingdom, especially when it comes to business or spy espionage incidents. Romantic or sexual relationships can be used by foreign agents or unscrupulous persons to influence targets for financial or political gain or to get sensitive information. Honey trapping crimes in the UK can vary from straightforward con games to more sophisticated schemes involving organised crime gangs. These occurrences frequently target powerful or rich people, manipulating them into vulnerable circumstances through charm, seduction, or trickery. The United Kingdom's law enforcement authorities employ several tactics to combat such offences, including as monitoring, clandestine operations, and educating the public about the potential hazards of interacting with unfamiliar individuals, particularly on the Internet (Chambre & Bloom, 2024).

Reports of honey trap crimes have surfaced in several Middle Eastern nations, sometimes with cultural or religious overtones (Amir, 2017). People who have extramarital romances or relationships that defy social conventions may become the victim of extortion or blackmail. The

consequences of getting trapped in a honey trap can be especially dire in conservative civilizations, such as the ones found in the Middle East, where social standards regarding relationships, gender roles, and sexuality can be rigid (Amir, 2017). Depending on the details of the case and the applicable national legislation, this might have both personal and legal ramifications. Like their counterparts worldwide, governments and security services in the Middle East are probably aware of the possibility of honey traps and may take action to warn people about the dangers and safeguard private data. They could also use counterintelligence techniques to find and eliminate these dangers (Amir, 2017).

The adoption of digital platforms and social media has had a profound impact on individuals, businesses, and organizations, fundamentally altering the way we communicate, consume information, and engage with the world around us (Boyd & Ellison, 2007; van Dijck, 2013). This study analyses the honey trapping crime cases to interrogate the methods and implication strategies of honey trapping, highlighting its transition from physical seduction to digital manipulation. It also scrutinizes the legal and ethical challenges posed by honey-trapping, emphasizing the lack of robust legal mechanisms to address these crimes. The increasing use of social media for honey trapping, entailing identity impersonation, and psychological manipulation, is critically analysed. Furthermore, the paper discusses preventive measures to equip individuals and organisations against such threats.

2. Honey Trapping Crime Cases in India

Different cases are reported in different parts of the country every year and criminal modus operandi is constantly adapting to the dynamic digital technology development. This study considers just four of those recently reported cases. *The Indian Express* reported a case in 2021 in which a bank officer in Mumbai became a victim of extortion and a cyber honey trapping, highlighting the risks associated with online contacts and the intelligence of hackers (Express News Service, 2021). The affair started as a harmless Facebook friend request but quickly turned into a financial loss and psychological suffering for the victim. The false identity used the recorded video to his advantage and demanded Rs 32,500 from the victim to stop the incriminating film from being released. The bank representative gave in to the pressure and paid the sum. But the story did not end there. While looking for information on cybercrime and complaints, he came across an online expert. The victim got a call from someone posing as a cyber expert after providing his information on the website, and this person promised to remove the video that implicated him. The video was asked to be removed from social media by the so-called experts for Rs 8,224, and from the blackmailer's phone and laptop for an extra Rs 26,000. Desperate to protect his image, the victim consented and paid Rs 34,224 in total. The bank official only realized he had been duped when the alleged cyber experts ceased communication with him after receiving the payment. Feeling betrayed and with no resolution in sight, he filed a complaint with the Andheri police on July 5th 2021. A First Information Report FIR was registered, and an investigation into the intricate web of online deception was initiated (Express News Service, 2021). This instance serves as a reminder of the risks associated with online impersonation and the extortion of sexual content. It emphasises how people should use caution while communicating on social networking sites and be mindful of the hazards involved in disclosing personal information online. Though it is not an easy task, users need a growing awareness of the cyber risks. The Mumbai police's examination of this cyber honey

trapping serves as a reminder of how cyber crimes are always changing and how crucial cyber-security knowledge is in the digital era. Information security awareness and training is a key factor. Human Firewall plays a complementary role in information security (Koza, 2022; Menear, 2024; Okumu et al., 2023).

The Indian Express reported another case in 2023. A highly respected Defence Research and Development Organisation (DRDO) officer was recently detained by the Maharashtra State Anti-Terrorism Squad (ATS) in Pune, India (Express News Service, 2023a). The individual is suspected of wrongful communication with intelligence agents headquartered in Pakistan, despite having been involved in many strategically important initiatives relating to missile development. The DRDO submitted a complaint, which resulted in the official's detention. The Official Secrets Act has been cited against the official. According to the investigation agency, the official was caught in a honeytrap set up by intelligence agents located in Pakistan who used images of women on social networking sites. Voice mails and video conversations are said to have been the senior scientist's means of communication with these agents during September and October. It is believed that he gave the foreign operatives crucial information on DRDO programmes during this time (Express News Service, 2023a). This case highlights the risks that anyone who has access to private information may run into, particularly in the era of social media and digital communication. The claimed usage of a honey trapping by foreign intelligence agents highlights how crucial it is to implement strict security measures, not only by technological means but also by regular tuition and pointers about contemporary cyber reconnaissance methods, to protect vital national assets and data. The degree of the official's involvement and the possible impact on national security will be determined via the judicial processes.

The Indian Express reported another case in 2023 that the Coimbatore City Cybercrime police recently busted a well-known group that was engaged in extortion and cyber fraud (Express News Service, 2023b). The gang, which had seven members, was based in Navi Mumbai, although its members were originally from Tamil Nadu. The group used honey trapping to entice gullible people into their complex plan. On October 15th, 2022, a 21-year-old Coimbatore college student replied to an online partner search ad, which led to the discovery of the case. In need of company, the victim got in touch with one of the group members, who assured her that he would set up massage and escort services at a Coimbatore hotel. Under several false pretences, including advance payment, room service, and safety precautions, the student was forced to pay Rs 7.84 lakh rupees. The victim informed the cybercrime police of the event after realising he had been duped. Following the hearing in the Mumbai court, the detained persons were sent to Coimbatore. Police are presently holding the suspects while legal processes are in progress. Sections 420 IPC and 66D of the IT Act, which deal with fraud and cheating online, are among the allegations brought against them (Express News Service, 2023b). This case serves as a reminder of the growing sophistication of cybercrimes and the value of law enforcement agencies working together to combat them. This makes it clear that despite of all forensic implications a cyber offender is not normally entirely able to veil his traces.

The Tribune reports a case that happened in the same year, 2023, that a clever plan utilising honey trapping has been used by a growing wave of cybercrime to target wealthy older men in the scenic state of Himachal Pradesh (Lohumi, 2023). The local police have received 55 complaints in the first two months of this year, which highlights a troubling trend that mixes extortion, manipulation, and technology. Cybercriminals use a methodical approach to trick their victims. They use WhatsApp to make the first contact with their carefully chosen targets, who

are mainly wealthy males between the ages of 45 and 75. Initial communication moves from phone conversations to text messages and video chats. The video calls are then recorded by the scammers, who then edit the footage to produce sexual videos. If a ransom is not paid, the scammers next threaten to post the edited footage online. Occasionally, victims get fictitious police notices on WhatsApp, requesting large sums of money as payment for alleged injuries to the women in the videos. The sums demanded for extortion vary from thousands to millions. The Additional Superintendent of Police (Cybercrime), brought attention to the fact that 97 % of complainants choose not to file complaints out of concern for societal stigma (Lohumi, 2023). 95 % of the 55 complaints concerned men between the ages of 45 and 75. He issued a warning about chatting with strangers on WhatsApp and disclosed that wealthy men were the target of scammers who conducted in-depth online research. Honey trapping techniques were used by the perpetrators, who were mostly school dropouts and illiterate teens from Mewat, Bharatpur, Alwar, and Nagar in Rajasthan, and Haryana (Lohumi, 2023). Only a small percentage of victims have come forward because of the pervasive societal shame and fear, which has hampered reporting. The victims have had to pay substantial amounts of money to stop the distribution of modified information, which has had a huge financial impact. To battle increasing cyber threats, the case emphasises the significance of cybersecurity awareness and the necessity of coordinated efforts between law enforcement authorities and the community. The case also delineates the enormous dark field of cyber crime in comparison to other crime phenomena.

3. Legal Concerns Around Honey Trapping Crimes

Honey trapping crimes pose a significant threat to national security, privacy, and individual well-being. India has implemented various legal frameworks to combat honey-trapping and safeguard its citizens. The Official Secrets Act of India prohibits the unauthorized possession, communication, or disclosure of information that could harm India's sovereignty, security, or relations with foreign states (*The Official Secrets Act*, 1923). Honey trapping activities that involve the leakage of sensitive information can be prosecuted under this act, with offenders facing severe penalties. Furthermore, the Information Technology Act plays a crucial role in addressing cyber-enabled honey trapping operations. The act criminalizes the publication of obscene or harassing content, the impersonation of others, and the hacking of computer systems (*The Information Technology Act*, 2000). These provisions help curb the use of electronic communication platforms for honey trapping crimes purposes. The Indian Penal Code, encompassing a wide range of offences, also serves as a legal safeguard against honey trapping. Blackmailing, extortion, and cheating, all of which can be employed in Honey trapping schemes, are punishable offences under this code (*Indian Penal Code*, 1860). These provisions protect individuals from being coerced or deceived into revealing sensitive information or engaging in acts that harm their interests. The Criminal Procedure Code establishes the procedures for criminal investigations and trials related to honey trapping. It ensures that the accused are afforded due process, including the right to a fair hearing and the presumption of innocence (*The Code Of Criminal Procedure*, 1973). This code helps maintain the integrity of the legal system and protects the rights of individuals involved in honey trapping cases. While these legal frameworks provide a solid foundation for combating honey trapping, enforcing

these laws can be challenging due to the clandestine nature of such operations and the reluctance of victims to come forward. Nonetheless, India's commitment to addressing honey-trapping through comprehensive legal frameworks demonstrates its dedication to safeguarding its citizens and upholding national security. So the dynamic character and the variability of cyber offences necessitate permanent adjustment of the penal code.

Honey trapping crimes pose a significant threat to national security in India. It can compromise sensitive information, undermine public trust in institutions, and jeopardize the integrity of national defence and security strategies. Honey trapping operations often target individuals with access to classified information, such as military personnel, government officials, and scientists. The leakage of this sensitive information can expose national defence plans, compromise intelligence operations, and provide foreign adversaries with a strategic advantage (Arcos et al., 2023; Borum et al., 2006; Hauer, 2015). Honey-trapping cases can erode public trust in government institutions, particularly those responsible for national security. The perception that individuals entrusted with sensitive information are vulnerable to manipulation can undermine public confidence in the government's ability to protect national interests (Dogan, 1997; Manny, 2007). Honey trapping can lead to the disruption and compromise of national security strategies. Foreign adversaries can exploit honey trapping operations to gain insights into India's defence plans, intelligence operations, and critical infrastructure vulnerabilities.

4. Suggestions for Effective Prevention

Preventing and countering honey trapping crimes requires a multifaceted approach that encompasses awareness, education, ethical guidelines, and robust legal frameworks. Raising awareness about honey trapping tactics is crucial for individuals, particularly those with access to sensitive information. Educational campaigns should highlight the common methods used by honey trappers, the potential consequences of falling victim to these tactics, and strategies for identifying and avoiding such situations. The Indian government and relevant organizations should launch public awareness campaigns to educate citizens about honey-trapping tactics, risks, and prevention measures. These campaigns can utilize various media channels, including television, radio, print, and online platforms. Individuals with access to sensitive information, such as government officials, military personnel, and scientists, should receive targeted education about honey trapping. This education can be provided through training programs, workshops, and seminars. As honey trapping often involves online interactions, educating individuals about cybersecurity practices is essential. This includes being cautious about online interactions, protecting personal information, and recognizing phishing attempts (Karabacak, 2014; Purpura, 2007). Building cyber resilience is a permanent task, from school to senior citizens.

Honey trapping crime cases pose significant ethical concerns in India. It violates the fundamental principles of trust, consent, and privacy, causing emotional distress, privacy violations, and harm to individuals and institutions. Addressing these ethical implications necessitates a multi-pronged approach that includes raising awareness among the public about honey trapping tactics, encouraging open communication and support for victims, promoting ethical values and integrity within organizations, and strengthening legal frameworks and enforcement mechanisms. Establishing clear ethical guidelines and fostering a culture of integrity within organizations, particularly those handling sensitive information, is essential. These guidelines

should explicitly prohibit honey trapping and emphasize the importance of maintaining professional boundaries and upholding ethical standards. Organizations should develop and implement comprehensive codes of conduct that clearly define honey-trapping as an offence and outline the consequences of engaging in such activities. Organizations should provide regular ethical training for employees, emphasizing the importance of ethical decision-making and personal responsibility. Leaders within organizations should set a strong example by adhering to ethical principles and demonstrating a commitment to preventing honey trapping (Somers, 2001).

Robust legal frameworks that deter and prosecute individuals involved in honey-trapping activities are crucial for effective prevention in India. Laws should clearly define honey trapping as an offence and provide for commensurate penalties. Additionally, law enforcement agencies should be equipped with the necessary training and resources to investigate and prosecute honey-trapping cases. Accompanying scientific expert knowledge is essential therefore alliances between government and police authorities. The Indian government should review and reform existing laws to ensure that honey-trapping is comprehensively addressed and that there are adequate deterrents and penalties for perpetrators. India should collaborate with international partners to share intelligence and best practices in addressing honey trapping, as this issue often transcends national borders (Hrebeniuk, 2019; Murphy, 2013).

Counterintelligence agencies in India play a critical role in identifying and neutralizing foreign intelligence operatives using honey-trapping techniques. These agencies should employ advanced surveillance techniques, monitor online activities, and maintain a network of trusted informants to uncover honey trapping operations. Counterintelligence agencies should actively collect and analyse intelligence related to honey-trapping activities, identifying patterns and potential threats. Advanced surveillance techniques, including electronic and digital monitoring, can help identify suspicious online interactions and potential honey trapping operations. Cultivating a network of trusted informants can provide valuable insights into honey trapping activities and enable timely interventions (Prunckun, 2011; Van Cleave, 2007).

Individuals who have fallen victim to honey trapping often experience emotional distress, trauma, and reputational damage. Providing accessible and confidential psychological support services can help victims cope with these challenges and facilitate their recovery. The Indian government or non-profit organizations should establish dedicated support centres for victims of honey trapping, providing psychological counselling, trauma therapy, and legal guidance. Victims of honey-trapping should be aware of available support services and encouraged to seek help without fear of stigma or judgment. Confidentiality and privacy protections should be paramount when providing support to victims, ensuring that their personal information is safeguarded (Dakof & Taylor, 1990; Gottfredson et al., 1987; Kaniasty & Norris, 1992).

5. Conclusion

The study serves as a stark reminder of the insidious nature of this practice and the urgent need to address it from multiple angles. It reveals how honey trappers, often operating under the guise of love or friendship, exploit individuals' vulnerabilities to gain access to sensitive information or influence their actions. The case study highlights the far-reaching impact of honey-trapping, which can lead to emotional distress, privacy violations, financial loss, repu-

tational damage, and even national security breaches. The study also underscores the importance of raising awareness about honey-trapping tactics and empowering individuals to protect themselves from this form of manipulation. Educating the public about the common methods used by honey trappers and encouraging open communication about suspicious online interactions, can help individuals safeguard their personal information and maintain healthy relationships. Furthermore, the study emphasizes the need for organizations to establish clear ethical guidelines and foster a culture of integrity to prevent honey-trapping from taking root within their ranks. By promoting ethical decision-making and personal responsibility, organizations can create a workplace where individuals feel safe and supported, minimizing the risk of honey-trapping infiltration. The legal framework surrounding honey-trapping is also crucial in deterring and prosecuting perpetrators. By enacting comprehensive laws that clearly define honey-trapping as an offence and provide commensurate penalties, combined with consistent outreach effort in suitable resolved cases, government can send a strong message that this behaviour will not be tolerated. Additionally, law enforcement agencies must be equipped with the necessary training and resources to effectively investigate and prosecute honey-trapping cases. Finally, the study proposes the need for psychological support services to help victims of Honey-trapping cope with the emotional distress, trauma, and reputational damage they may experience. By providing accessible and confidential counselling and therapy, we can help victims heal and reclaim their lives. Only through collective action can we protect our society from the harmful effects of this clandestine manipulation.

References

Amir, S. Al. (2017). *Dubai honey trap gang of women 'beat up clients and stole their money*.' N UAE. https://www.thenationalnews.com/uae/courts/dubai-honey-trap-gang-of-women-beat-up-clients-and-stole-their-money-1.627333 (2024, May 9).

Arcos, R., Chiru, I., & Ivan, C. (2023). *Routledge Handbook of Disinformation and National Security*. Routledge. https://doi.org/10.4324/9781003190363

Borum, R., Shumate, R. S., & Scalora, M. (2006). Psychology of Leaking Sensitive Information: Implications for Homeland Security. *Homeland Security Review*, *1*(2), 97.

Boyd, D. M., & Ellison, N. B. (2007). Social Network Sites: Definition, History, and Scholarship. *Journal of Computer-Mediated Communication*, *13*(1), 210–230. https://doi.org/10.1111/j.1083-6101.2007.00393.x

Chambre, A., & Bloom, D. (2024). *Police launch inquiry into UK parliament 'honey trap' sexting scandal*. Politico. https://www.politico.eu/article/westminster-online-scam-police-launch-inquiry-into-uk-parliament-honey-trap-scandal/#:~:text=POLITICO revealed Wednesday at least,in several cases naked photos.&text=LONDON — British police have launched,complaint from a se (2024, May 9).

Dakof, G. A., & Taylor, S. E. (1990). Victims' perceptions of social support: What is helpful from whom? *Journal of Personality and Social Psychology*, *58*(1), 80–89. https://doi.org/10.1037/0022-3514.58.1.80

Dalmia, V. (2019, October 23). Escaping the Honey Trap: How India can deal with an age-old spy craft that has been reinvented for the digital age. *The Hindu*. https://www.thehindu.com/opinion/op-ed/escaping-the-honey-trap/article29771225.ece (2024, May 10).

Dalrymple, W. (2002). *White Mughals: Love and Betrayal in Eighteenth-Century India*. Penguin Books.

Deuskar, N. (2023, July 12). Pakistani Spies are Honey-Trapping India's Scientists and Soldiers by Pretending to be Women Online. *Scroll.In*. https://scroll.in/article/1052396/pakistani-spies-are-honey-trapping-india-s-scientists-and-soldiers-by-pretending-to-be-women-online (2024, May 10).

Dogan, M. (1997). Erosion of confidence in advanced democracies. *Studies in Comparative International Development*, *32*(3), 3–29. https://doi.org/10.1007/BF02687328

Express News Service. (2021, July 7). Mumbai: Honey trap victim duped by 'cyber expert' he approached for help. *The Indian Express*. https://indianexpress.com/article/cities/mumbai/mumbai-honey-trap-victim-duped-by-cyber-expert-he-approached-for-help-7392852/ (2024, May 9).

Express News Service. (2023a, May 5). Senior DRDO official held in suspected honey trap case with Pakistan links. *The Indian Express*. https://indianexpress.com/article/cities/pune/senior-drdo-official-arrest-honey-trap-case-pakistan-links-8592089/ (2024, May 10).

Express News Service. (2023b, June 12). Honey trapping: Coimbatore cybercrime police arrest seven-member gang from Navi Mumbai. *The New Indian Express*. https://www.newindianexpress.com/states/tamil-nadu/2023/jun/12/honey-trapping-coimbatore-cybercrime-police-arrest-seven-member-gang-from-navi-mumbai-2584067.html#:~:text=COIMBATORE%3A A gang of seven,Coimbatore City Cybercrime police recently (2024, May 10).

Firstpost. (2022). *USA: Sextortion cases rise by 1,000 per cent in 2022, kids at maximum risk*. Firstpost. https://www.firstpost.com/world/usa-sextortion-cases-rise-by-1000-per-cent-in-2022-kids-at-maximum-risk-11841281.html (2024, May 11).

Gottfredson, G. D., Reiser, M. & Tsegaye-Spates, C. R. (1987). Psychological help for victims of crime. *Professional Psychology: Research and Practice*, *18*(4), 316–325. https://doi.org/10.1037/0735-7028.18.4.316

Gupta, D. (2023). *Honey Trap – The Crime*. Reflections. https://reflections.live/articles/11031/honey-trap-the-crime-an-article-by-deepa-gupta-9997-lipuclgc.html#:~:text=Shining the Light on the Great Indian Honey Trap%3A&text=During the Cold War%2C intelligence,into giving away valuable secrets. (2024, May 9).

Hauer, B. (2015). Data and Information Leakage Prevention Within the Scope of Information Security. *IEEE Access*, *3*, 2554–2565. https://doi.org/10.1109/ACCESS.2015.2506185

Honey Trap: The New Espionage Outfit. (2023). Innefu Labs. https://www.innefu.com/blog/honey-trap-the-new-espionage-outfit/. (2024, May 11).

Hrebeniuk, M. V. (2019). The directions of improving the legislative framework in the sphere of supply state security in the vector-fight against organized crime. *Публічне Урядування*, *4*, 78–91.

Indian Penal Code. (1860). Government of India. https://github.com/civictech-India/Indian-Law-Penal-Code-Json

Innefu. (2023). *Honey Trap: The New Espionage Outfit*. Innefu Labs. https://www.innefu.com/blog/honey-trap-the-new-espionage-outfit/.

Kaniasty, K., & Norris, F. H. (1992). Social support and victims of crime: Matching event, support, and outcome. *American Journal of Community Psychology*, *20*(2), 211–241. https://doi.org/10.1007/BF00940837

Karabacak, B. (2014). Strategies to Counter Cyberattacks: Cyberthreats and Critical Infrastructure Protection. *Critical Infrastructure Protection*, *116*, 63.

Kinsale, N. (2023). *The Art of Honey Trapping: Unveiling the Secrets of Private Investigators*. Linkedin.Com. https://www.linkedin.com/pulse/art-honey-trapping-unveiling-secrets-private-natalie-kinsale/ (2024, May 12).

Koza, E. (2022). *Information Security Awareness and Training as a Holistic Key Factor – How Can a Human Firewall Take on a Complementary Role in Information Security?* https://doi.org/10.54941/ahfe1002201

Kumara, S. S., Chandrab, R., & Agarwal, S. (2024). Rule based Complex Event Processing for an Air Quality Monitoring System in Smart City. *ArXiv Preprint ArXiv:2403.14701*. https://arxiv.org/abs/2403.14701 (2024, May 12).

Lindley, M. (2023). *The Four Cybersecurity Trends to Watch in 2023*. Cybersecurity- Iniders.Com. https://www.cybersecurity-insiders.com/the-four-cybersecurity-trends-to-watch-in-2023/ (2024, May 12).

Lohumi, B. P. (2023, March 27). Cyber fraudsters lure Himachal Pradesh's elderly men into honey trap. *The Tribune*. https://www.tribuneindia.com/news/himachal/cyber-fraudsters-target-himachal-pradeshs-elderly-men-381307 (2024, May 12).

Mandarin, G. T. for R. (2024). *China's state security ministry issues lurid 'honey trap' warning*. Radio Free Asia. https://www.rfa.org/english/news/china/honey-trap-01232024141917.html (2024, May 12).

Manny, C. (2007). Is the US Government's Mining of Commercial Data Contributing to an Erosion of Public Trust in Government? *Forum on Public Policy Online*. https://forumonpublicpolicy.com/%0Aarchivesum07/manny.pdf (2024, May 9).

Menear, R. (2024). Building a human firewall to keep your organisation secure. *Network Security*, *2024*(5). https://doi.org/10.12968/S1353-4858(24)70019-1

Murphy, R. (2013). *Peace Operations and Human Rights*. Routledge. https://doi.org/10.4324/9781315878836

Nosál, J. (2023). Crime in the Digital Age: A New Frontier. In *The Implications of Emerging Technologies in the Euro-Atlantic Space* (pp. 177–193). Springer International Publishing. https://doi.org/10.1007/978-3-031-24673-9_11

Okumu, D. O., Omollo, R. O., & Raburu, G. (2023). Human Firewall Simulator for Enhancing Security Awareness against Business Email Compromise. *Journal of Computational and Cognitive Engineering*. https://doi.org/10.47852/bonviewJCCE3202415

OpIndia. (2024). *Russians cannot use honeytrap against French spies because 'their wives already know about their affairs': Reveals documentary on DGSE*. OpIndia. https://www.opindia.com/2024/04/russians-cannot-use-honeytrap-against-french-spies-because-their-wives-already-know/ (2024, May 9).

Prunckun, H. (2011). A Grounded Theory of Counterintelligence. *American Intelligence Journal*, *29*(2), 6–15.

Purpura, P. (2007). *Security and loss prevention: An Introduction*. Butterworth-Heinemann.

Sawant, G. C. (2019, January 20). Indian Army Takes Steps to Prevent Honey-trapping of Soldiers by ISI Operatives. *India Today*. https://www.indiatoday.in/mail-today/story/indian-army-takes-steps-to-prevent-honey-trapping-of-soldiers-by-isi-operatives-1434829-2019-01-20 (2024, May 9).

Somers, M. J. (2001). Ethical Codes of Conduct and Organizational Context: A Study of the Relationship Between Codes of Conduct, Employee Behavior and Organizational Values. *Journal of Business Ethics*, *30*, 185–195. https://doi.org/https://doi.org/10.1023/A:1006457810654

The Code Of Criminal Procedure. (1973). Government of India. https://www.indiacode.nic.in/bitstream/123456789/4221/1/Criminal-Procedure-Code-CrPC-1973.pdf (2024, May 10).

The Information Technology Act. (2000). Ministry of Law and Justice, Government of India. https://lddashboard.legislative.gov.in/actsofparliamentfromtheyear/information-technology-act-2000 (2024, May 10).

The Official Secrets Act. (1923). Government of India. https://www.indiacode.nic.in/bitstream/123456789/2379/1/A1923-19.pdf (2024, May 11).

Van Cleave, M. K. (2007). *Counterintelligence and National Strategy*. https://apps.dtic.mil/sti/pdfs/ADA471485.pdf (2024, May 11).

van Dijck, J. (2013). *The Culture of Connectivity*. Oxford University Press. https://doi.org/10.1093/acprof:oso/9780199970773.001.0001

Kontakt | Contact

Pranav Prakash | Department of Criminology | Karunya Institute of Technology and Sciences | pranavprakash750@gmail.com

Surbhi Girdhar | Department of Criminology | Karunya Institute of Technology and Sciences | girdharsurbhi89@gmail.com

Antony Jose | PG Department of English | Naipunnya Institute of Management and Information Technology | frantony@naipunnya.ac.in